AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO. | 1. CONTRACT ID CODE | PAGE 1 | OF PAGES 82

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NUMBER	5. PROJECT NUMBER (if applicable)
A00001			

6. ISSUED BY CODE

Attn: Juan Quinones, Contracting Officer
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

7. ADMINISTERED BY (If other than Item 6) CODE

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)

To all Offerors/Bidders

CODE | FACILITY CODE

(X) | 9A. AMENDMENT OF SOLICITATION NUMBER: VA118-17-R-1848

X | 9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NUMBER

10B. DATED (SEE ITEM 13)

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

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

(a) By completing Items 8 and 15, and returning 1 copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

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

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

E. IMPORTANT: Contractor [ ] is not, [ ] is required to sign this document and return _____ copies to the issuing office.

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

See Continuation Page

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

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

CONTINUATION PAGE

The purpose of this Amendment A00001, to Request for Proposal (RFP) VA118-17-R-1848 titled "Faster Care for Veterans Pilot Program," is as follows:

1. Section B.6, Rights in Computer Software is hereby incorporated.

2. Section B.7 Schedule of Deliverables:
    a. SLINs 0004AA, 0004AB, 0004AC, 1002AA, 1002AB, 1002AC, 2002AA, 2002AB, and 2002AC are hereby incorporated to price the OPSS Licenses and Hosting per VA facility.

3. Section B.7 Performance Work Statement (PWS):

    a. Paragraph 2.0 Applicable Documents: Included VA Handbook 6517, Risk Management Framework For Cloud Computing Services, dated November 15, 2016
    b. Paragraph 5.3 OPSS Startup and Configuration: #9 is hereby revised from "For Mental Health, the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months to "For Mental Health and Specialty Care, the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months."
    c. Paragraph 5.3 OPSS Startup and Configuration: #11 is hereby revised to include the requirement for the Contractor to retain Right of Access forms throughout the PoP and transition them to VA at the conclusion of the contract.
    d. Paragraph 5.4 VA System Integration and Interface Development: #11 is hereby revised to include the requirement for the Contractor to maintain patient access logs through the PoP and transition them to VA at the conclusion of the contract. Paragraph 5.4 VA System Integration and Interface Development: #13 is hereby revised from "Capable of integrating with VistA using VA-approved web services, remote procedure calls (RPC), and security standards, etc." to "Capable of integrating with VistA using VA provided middleware/application programming interfaces, remote procedure calls (RPC), and security standards, etc."
    e. Paragraph 5.5 Pilot Project Operation and Evaluation Support: Revised to include "The Contractor shall provide the hosting, licenses/Software as a Service (SaaS) as applicable to the commercial product proposed."
    f. Paragraph 5.5 Pilot Project Operation and Evaluation Support: Revised the number of provider participants in the pilot per VA facility.
    g. Paragraph 5.5 Pilot Project Operation and Evaluation Support: Revised from "The user base for the pilot test shall include every patient who has had an appointment at the pilot site within the last 13 months to "The user base for the pilot test shall include every patient who has had an appointment at the pilot site within the last 13 months in Mental Health or Specialty Care or are assigned a Primary Care Provider."
    h. Paragraph 5.7.4: Examples of incidents are hereby incorporated. "The Contractor shall coordinate appropriate resources to address incidents (e.g.

functional errors, availability/uptime, accessibility and security incidents) and communicate incident related information for situational awareness within two hours of the incident to the COR and VA PM."

4. Section E.12 Proposal Submission:
    a. Volume I Technical at E.12(2)(c): The Page limitation is hereby increased from 20 pages to 25 pages.
    b. Volume 1 Technical Factor at E.12(2)(c)(i)(2): Corrected enumeration.
    c. Volume 1 Technical Factor at E.12(2)(c)(i)(2): #9 is hereby revised from "For Mental Health, the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months to "For Mental Health and Specialty Care, the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months."
    d. Volume II Past Performance Factor at E.12(2)(c)(ii): Revised from "Offerors shall submit a list of all contracts (including Federal, State, and local government and private) (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation" to "Offerors shall submit up to 10 contracts (including Federal, State, and local government and private) (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation."

5. Attachment 002 – Price Schedule Excel Spreadsheet:
    a. CLIN 0004 is hereby revised from LO to MO
    b. SLINs 0004AA, 0004AB, 0004AC, 1002AA, 1002AB, 1002AC, 2002AA, 2002AB, and 2002AC are hereby incorporated to price the OPSS Licenses and Hosting per VA facility.

6. The solicitation is hereby extended to close on March 6, 2017 12:00PM EST.

7. Except as provided herein, all other terms and conditions of RFP VA118-17-R-1848 remain unchanged and in full force and effect.

B.6 RIGHTS IN COMPUTER SOFTWARE

The Contractor is required to deliver technical data, configurations, documentation or other information, including source code, during contract performance in accordance with Contract Line Item Number (CLIN 0003). The Government shall receive Unlimited Rights in intellectual property first produced and delivered in the performance of this contract in accordance with FAR 52.227-14, Rights In Data-General (MAY 2014). This includes all rights to source code and any and all documentation created in support thereof. License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, Commercial Computer Software License (DEC 2007).

B.7 PRICE SCHEDULE

Inspection/Acceptance//F.O.B: Destination.

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

The Price Schedule contains contract line items identified as not separately priced (NSP). This means the price for the line item is included in the price of another, related line item. The Contractor shall not invoice the Government for any portion of the contract line item which contains an NSP until the Contractor has delivered the total quantity of all related contract line items and the Government has accepted them.

BASE PERIOD					
CONTRACT LINE ITEM NUMBER (CLIN)	**DESCRIPTION**	**QTY**	**UNIT**	**UNIT PRICE**	**TOTAL PRICE**
0001	Project Management in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1, inclusive of subparagraphs 5.1.1 through 5.1.8; PWS paragraph 6.2.2; and PWS Addendum A paragraph A3.4. This CLIN includes all tasks, labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1 inclusive of subparagraphs 5.1.1 through 5.1.8; PWS paragraph 6.2.2; and PWS Addendum A paragraph A3.4 for the base period and each option period and optional task, if exercised. The price of Project Management CLIN 0001 including SLINs 0001AA through 0001AK shall be included in and allocated to CLINs 0003 through 0006 and if exercised, 1001 through 1004; 2001 through 2004; 3001; 4001; 4002; and 5001. Period of Performance (PoP) shall be	18	MO	NSP	NSP

	18 months after contract award.				
0001AA	Contractor Project Management Plan (CPMP) IAW PWS paragraph 5.1.1 The initial baseline CPMP shall be submitted 30 days after contract award (DACA) and updated no later than five days after receipt of VA comments. Updated monthly thereafter. Electronic submission to: VA PM, COR, Contracting Officer (CO)	1	LO	NSP	NSP
0001AB	Monthly Progress Report IAW PWS paragraph 5.1.3 Due the 5th day of each month throughout the PoP. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AC	Rational Training Certificates IAW PWS paragraph 5.1.4 Due within 14 days of the identification of the need for access to Rational Tool Suite. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AD	VA Privacy and Information Security Awareness and Rules of Behavior Training Certificates IAW PWS paragraph 5.1.5 Due 30 DACA. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AE	Signed Contractor Rules of Behavior IAW PWS paragraph 5.15 Due 30 DACA. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AF	VA HIPAA Certificates of Completion IAW PWS paragraph 5.1.5 Due 30 DACA. Electronic submission to: VA PM,	1	LO	NSP	NSP

	COR, CO				
0001AG	Onboarding Status Reports IAW PWS paragraph 5.1.6 Due 10 DACA and updated weekly on Friday until onboarding is complete. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AH	Configuration Management Plan IAW PWS paragraph 5.18 Due 30 DACA and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AI	Version Description Document IAW PWS paragraph 5.1.8 Due at each project build delivery with final draft due 10 days prior to build release. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AJ	Contractor Staff Roster IAW PWS paragraph 6.2.2 Due three business DACA and updated within five days of Contractor Staff Roster change. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0001AK	Final Section 508 Compliance Test Results IAW PWS Addendum A paragraph A3.4. Due six months after award for the OPSS solution and upon delivery of each deliverable. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002	Veteran-focused Integration Process (VIP) Development Lifecycle IAW PWS paragraph 5.2, inclusive of subparagraphs 5.2.1 through 5.2.2.6	18	MO	NSP	NSP

	This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2 and all of its subparagraphs for the base period and each option period and optional task, if exercised. The price of VIP Development Lifecycle CLIN 0002 and SLINs 0002AA through 0002AK shall be included in and allocated to CLIN 0003 and if exercised, 3001. PoP shall be 18 months after contract award.				
0002AA	System Design Document and Updates IAW PWS paragraph 5.2.2.1 Due 10 days prior to the start of first sprint and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AB	Build Plans IAW PWS paragraph 5.2.2.2 Due 10 days prior to the start of each build. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AC	Project Backlogs IAW PWS paragraph 5.2.2.2 Due 10 days prior to the start of each build and updated at the end of each build. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AD	Sprint Plan IAW PWS paragraph 5.2.2.3 Due at the start of each sprint and updated as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP

0002AE	Source Code and Rational Updates IAW PWS paragraph 5.2.2.4 Updated daily to Rational with final versions due at the delivery of each build. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AF	Test Strategy Data IAW PWS paragraph 5.2.2.5 Due 10 days prior to the start of the first sprint for each build and updated for each new build as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AG	Test Plan IAW PWS paragraph 5.2.2.5 Final due 10 days prior to build release. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AH	Test Script IAW PWS paragraph 5.2.2.5 Due five days after build start and updated weekly during sprints. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AI	Test Execution Data IAW PWS paragraph 5.2.2.5 Due daily in the Data Repository with final versions due three days prior to build release. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0002AJ	Test Results and Defect Logs IAW PWS paragraph 5.2.2.5 Due daily in the Data Repository with final versions due three days prior to build release. Electronic submission to: VA PM,	1	LO	NSP	NSP

	COR, CO				
0002AK	Build Acceptance Form IAW PWS paragraph 5.2.2.6 Due five days after completion of each Build or monthly for Pilot Operations support in accordance with PWS Task 5.5, Pilot Project Operation and Evaluation Support. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003	Software Development Lifecycle Scrum Team IAW PWS paragraph 5.3 - Online Patient Self-scheduling System (OPSS) Start-up and Configuration; 5.4 - VA System Integration and Interface Development and 5.5 - Pilot Project Operation and Evaluation Support. This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.3, 5.4, and 5.5 including its subparagraph. This excludes CLIN 0004 for OPSS licenses and hosting IAW PWS paragraph The Contractor shall only invoice upon COR acceptance of the Build Acceptance Form for the number of months it took to complete the build (i.e. Build complete in 2 months: contractor invoices monthly price x 2 months) or monthly for support of pilot operations. PoP shall be 18 months after contract award.	18	MO	$	$
0003AA	Assessment and Authorization (A&A) Package for the OPSS IAW PWS paragraph 5.5.1 Due no later than (NLT) six months after contract award and updated as required. Electronic submission to: VA PM,	1	LO	NSP	NSP

	COR, CO				
0003AB	A&A Package for the OPSS Cloud Hosting Facility IAW PWS paragraph 5.5.1 Due NLT six months after contract award and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AC	Pilot Strategy and Plan Document IAW PWS paragraph 5.5.2 Due 30 DACA and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AD	Training Materials IAW PWS paragraph 5.5.3 Due 10 days prior to pilot initiation and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AE	Knowledge Base Repository IAW PWS paragraph 5.5.3 Due 10 days prior to pilot initiation and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AF	Updated Production Operations Manual IAW PWS paragraph 5.5.4 Due 10 days prior to Critical Decision 2 (CD2) review and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AG	Updated Technical Manual IAW PWS paragraph 5.5.4 Due 10 days prior to CD2 review and updated as required.	1	LO	NSP	NSP

	Electronic submission to: VA PM, COR, CO				
0003AH	Updated User Manual IAW PWS paragraph 5.5.4 Due 10 days prior to CD2 review and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AI	Updated Version Description Document IAW PWS paragraph 5.5.4 Due 10 days prior to CD2 review and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AJ	Final Source and Executable Code IAW PWS paragraph 5.5.4 Due 10 days after pilot completion. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AK	Pilot Test Evaluation Report IAW PWS paragraph 5.5.5 Due the 5th of each month after pilot start. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AL	Pilot Exit Review IAW PWS paragraph 5.5.5 Due 10 days before pilot completion. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0003AM	Open Source Submission Package IAW PWS paragraph 5.5.6 Due 30 days after each code release and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP

0004	OPSS Licenses and Hosting IAW PWS paragraph 5.5.4 ~~Due NLT 10 days after CD2 decision.~~ The PoP shall be for a not to exceed (NTE) period of 18 months. ~~OPSS licenses and hosting are due 10 days after CD2 decision and shall co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months of Licenses and Hosting during pilot operations.~~ ~~Electronic submission to: VA PM, COR, CO~~	NTE 18	MO	~~-$~~	~~$-~~
0004AA	OPSS Licenses and Hosting IAW PWS paragraph 5.5.4 (Minneapolis, MN) Due NLT 10 days after CD2 decision. The PoP shall be for a NTE period of 18 months. OPSS licenses and hosting are due 10 days after CD2 decision and shall co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months of Licenses and Hosting during pilot operations. Electronic submission to: VA PM, COR, CO	NTE 18	MO	$	$
0004AB	OPSS Licenses and Hosting IAW PWS paragraph 5.5.4 (Bedford, MA) Due NLT 10 days after CD2 decision. The PoP shall be for a NTE period of 18 months. OPSS licenses and hosting are due 10 days after CD2 decision and shall co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months of Licenses and Hosting during pilot operations. Electronic submission to: VA PM, COR, CO	NTE 18	MO	$	$

0004AC	OPSS Licenses and Hosting IAW PWS paragraph 5.5.4 (Salt Lake City, UT) Due NLT 10 days after CD2 decision. The PoP shall be for a NTE period of 18 months. OPSS licenses and hosting are due 10 days after CD2 decision and shall co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months of Licenses and Hosting during pilot operations. Electronic submission to: VA PM, COR, CO	NTE 18	MO	$	$
0005	Help Desk Support IAW PWS paragraph 5.6. This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6. The PoP shall not exceed 18 months. Help Desk Support shall commence upon delivery of the OPSS licenses and hosting (0004) and co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months Help Desk Support is provided. If help desk support is included in the license and hosting price please indicate that the price of helpdesk support is included in CLIN 0004 and enter $0 for this CLIN.	NTE 18	MO	$	$
0006	OPSS Operations and Maintenance (O&M) IAW PWS paragraph 5.7. This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, including its subparagraph. The PoP shall not exceed 18 months. O&M shall commence upon delivery of	18	MO	$	$

	the OPSS licenses and hosting (0004) and co-term with the expiration of the base period. The Contractor shall invoice monthly based on the actual number months O&M is provided.				
0006AA	O&M Plan IAW PWS paragraph 5.7 Due 45 days after DACA and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0006AB	Performance Management Plan IAW PWS paragraph 5.7.2 Due 120 DACA and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
0006AC	Continuity of Operations (COOP)/ Disaster Recovery (DR) Plan IAW PWS paragraph 5.7.3 Due 45 DACA and updated as required. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
				Base Total	**$**

OPTION PERIOD 1

This option period may be exercised IAW FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence immediately after expiration of the base period.

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
1001	Pilot Project Operation and Evaluation Support – IAW PWS paragraph 5.8. This CLIN includes all program management (CLIN 0001), labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.5 including its subparagraph.	6	MO	$	$

	PoP shall be six months after exercise of option.				
1001AA	A&A Package for the OPSS IAW PWS paragraph 5.5.1 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
1001AB	A&A Package for the OPSS Cloud Hosting Facility IAW PWS paragraph 5.5.1 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
1001AC	Pilot Test Evaluation Report IAW PWS paragraph 5.5.5 Due the 5th of each month. . Electronic submission to: VA PM, COR, CO	6	MO	NSP	NSP
1001AD	Pilot Exit Review IAW PWS paragraph 5.5.5 Due 10 days before the expiration of the option period. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
1002	OPSS licenses and hosting IAW PWS paragraph 5.5.4 ~~Due upon exercise of option period.~~ ~~Electronic submission to: VA PM, COR, CO~~	6	MO	~~$-~~	~~$-~~
1002AA	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Minneapolis, MN) Due upon exercise of option period. Electronic submission to: VA PM, COR, CO	6	MO	$	$
1002AB	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Bedford, MA)	6	MO	$	$

	Due upon exercise of option period. Electronic submission to: VA PM, COR, CO				
1002AC	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Salt Lake City, UT) Due upon exercise of option period. Electronic submission to: VA PM, COR, CO	6	MO	$	$
1003	Help Desk Support IAW PWS paragraph 5.6. This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6 for the base period and each option period and optional task, if exercised. PoP shall be 6 months after exercise of option.	6	MO	$	$
1004	OPSS Operations and Maintenance IAW PWS paragraph 5.7. This CLIN includes all labor and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, including its subparagraph, for the base period and each option period and optional task, if exercised. PoP shall be 6 months after exercise of option.	6	MO	$	$
1004AA	O&M Plan IAW PWS paragraph 5.7 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
1004AB	Performance Management Plan IAW PWS paragraph 5.7.2 Update as needed. Electronic submission to: VA PM, COR,	1	LO	NSP	NSP

	CO				
1004AC	COOP/DR Plan IAW PWS paragraph 5.7.3 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
				Option Period 1 Total	**$**

OPTION PERIOD 2 **This option period may be exercised IAW FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer. If exercised, this option shall commence immediately after expiration of the base period.**					
CLIN	**DESCRIPTION**	**QTY**	**UNIT**	**UNIT PRICE**	**TOTAL PRICE**
2001	Pilot Project Operation and Evaluation Support – IAW PWS paragraph 5.8. This CLIN includes all program management (CLIN 0001), labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.5 including its subparagraph. PoP shall be six months after exercise of option.	6	MO	$	$
2001AA	A&A Package for the OPSS IAW PWS paragraph 5.5.1 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
2001AB	A&A Package for the OPSS Cloud Hosting Facility IAW PWS paragraph 5.5.1 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
2001AC	Pilot Test Evaluation Report IAW PWS paragraph 5.5.5 Due the 5th of each month.				

	Electronic submission to: VA PM, COR, CO	6	MO	NSP	NSP
2001AD	Pilot Exit Review IAW PWS paragraph 5.5.5 Due 10 days before the expiration of the option period. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
2002	OPSS licenses and hosting IAW PWS paragraph 5.5.4 ~~Due upon exercise of option period.~~ ~~Electronic submission to: VA PM, COR, CO~~	6	MO	~~$-~~	~~$-~~
2002AA	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Minneapolis, MN) Due upon exercise of option period. Electronic submission to: VA PM, COR, CO	6	MO	$	$
2002AB	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Bedford, MA) Due upon exercise of option period. Electronic submission to: VA PM, COR, CO	6	MO	$	$
2002AC	OPSS licenses and hosting IAW PWS paragraph 5.5.4 (Salt Lake City, UT) Due upon exercise of option period. Electronic submission to: VA PM, COR, CO	6	MO	$	$
2003	Help Desk Support IAW PWS paragraph 5.6. This CLIN includes all labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6 for the base period and each option period and optional task, if exercised.	6	MO	$	$

	PoP shall be 6 months after exercise of option.				
2004	OPSS Operations and Maintenance IAW PWS paragraph 5.7. This CLIN includes all labor and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, including its subparagraph, for the base period and each option period and optional task, if exercised. PoP shall be 6 months after exercise of option.	6	MO	$	$
2004AA	O&M Plan IAW PWS paragraph 5.7 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
2004AB	Performance Management Plan IAW PWS paragraph 5.7. Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
2004AC	COOP/DR Plan IAW PWS paragraph 5.7.3 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
				Option Period 2 Total	**$**

OPTIONAL TASK 1 - ADDITIONAL SCRUM TEAM SUPPORT In accordance with FAR 52.217-7, "Option for Increased Quantity-Separately Priced Line Item", this optional CLIN may be exercised no more than seven times throughout the period of performance. Delivery shall be in accordance with the Schedule.					
CLIN	**DESCRIPTION**	**QTY**	**UNIT**	**UNIT PRICE**	**TOTAL PRICE**
3001	**OPTIONAL TASK 1:** Additional Scrum Team Support IAW PWS paragraph 5.9. This CLIN includes all program management, labor, travel and deliverables required for the successful	NTE 78	MO	$	$

	completion of the services detailed in PWS paragraph 5.3, 5.4, 5.5 including its subparagraph. The scrum team shall follow the VIP, VA system integration and pilot processes described in Sections 5.2 through 5.5 of this PWS and shall adjust deliverables identified in CLINs 0002 and 0003 to match the nature of the software product under development. This task may be exercised no more than seven times throughout the PoP (it is estimated that the optional task may be exercised three times during the base period and two times in each option period NTE a total of 78 months). Each exercise is for one additional scrum team. Exercise of this optional task shall not exceed period of performance of the contract beyond 30 months. The Contractor shall price the Scrum Team on a monthly basis. The Contractor shall only invoice upon COR acceptance of the Build Acceptance Form for the number of months it took to complete the build. (i.e. Build complete in 2 months contractor invoices monthly price x 2 months)				
				TOTAL OPTIONAL TASK 1	**$**

OPTIONAL TASK 2 – LICENSES FOR INSTALLATION AT ADDITIONAL SITES

In accordance with FAR 52.217-7, "Option for Increased Quantity-Separately Priced Line Item", this optional CLIN may be exercised for increments of one additional site up to five times throughout the period of performance for a total of five sites. Delivery shall be in accordance with the Schedule.

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
4001	**OPTIONAL TASK 2:** Licenses/Hosting for Installation at Additional Sites IAW PWS paragraph 5.10 Due 10 days after exercise of optional task.	NTE 150	MO	$	$

	This optional task may be exercised for a total of five additional sites. The optional task can be exercised no more than 15 times to accommodate the procurement of licenses and/or renewals throughout the period of performance. The NTE number of months for licensing and hosting is 150 months. Exercise of this optional task shall not exceed period of performance of the contract beyond 30 months. The Contractor shall price the licenses and hosting on a monthly basis to be prorated based on actual pilot operations.				
4002	OPSS O&M IAW PWS paragraph 5.7 and 5.9. This CLIN includes all program management, labor, travel and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, including its subparagraph, for the base period and each option period and optional task, if exercised. The PoP shall not exceed 150 months. O&M shall commence upon delivery of the OPSS licenses and hosting (4001) for the duration of the license term. The Contractor shall invoice monthly based on the actual number months O&M is provided.	NTE 150	MO	$	$
4002AA	O&M Plan IAW PWS paragraph 5.7 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
4002AB	Performance Management Plan IAW PWS paragraph 5.7.2 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
4002AC	COOP/DR Plan IAW PWS paragraph				

	5.7.3 Update as needed. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
				TOTAL OPTIONAL TASK 2	**$**

OPTIONAL TASK 3 – TRANSITION SUPPORT **In accordance with FAR 52.217-7, "Option for Increased Quantity-Separately Priced Line Item", this optional CLIN may be exercised a single time, at any time during the period of performance. Delivery shall be in accordance with the Schedule.**					
CLIN	**DESCRIPTION**	**QTY**	**UNIT**	**UNIT PRICE**	**TOTAL PRICE**
5001	**OPTIONAL TASK 3:** Transition Support IAW PWS paragraph 5.11 If exercised, the period of performance shall be 60 days after exercise of the optional task.	1	LO	$	$
5001AA	Transition Plan IAW PWS paragraph 5.11 Due 10 days after exercise of optional task. Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP
				TOTAL OPTIONAL TASK 3	**$**
				TOTAL CONTRACT	**$**

B.8 PERFORMANCE WORK STATEMENT

PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology

Faster Care for Veterans Pilot Program

Date: February ~~7~~22, 2017
TAC-17- 41312
Version Number: ~~13~~14.0

1.0 BACKGROUND

On December 16, 2016 House Resolution 4352 (Public Law (PL) 114-286), "Faster Care for Veterans Act of 2016" was enacted directing the VA to carry out a pilot program in not less than three Veterans Integrated Services Networks (VISN) to evaluate the capability of an existing commercially available, off-the-shelf online patient self-scheduling system to schedule and confirm medical appointments in accordance with the seven congressionally mandated requirements at Section 3(a). This PWS is issued in support of that legislation.

PL 114-286 requires an existing commercially available system that provides Veterans the ability to use an Internet website and mobile application to schedule and confirm medical appointments at VA medical facilities. The solution shall provide the capability to run on the operating system of a cellular telephone, tablet computer, or similar portable computing device that transmits data over a wireless connection. The seven congressionally mandated requirements are:

1. Capabilities to schedule, modify, and cancel appointments for primary care, specialty care, and mental health.
2. Capability to support appointments for the provision of health care regardless of whether such care is provided in person or through telehealth services.
3. Capability to view appointment availability in real time.
4. Capability to make available, in real time, appointments that were previously filled but later cancelled by other patients.
5. Capability to provide prompts or reminders to Veterans to schedule follow-up appointments.
6. Capability to be used 24 hours per day, 7 days per week.
7. Capability to integrate with the Veterans Health Information Systems and Technology Architecture (VistA) of the Department, or such successor information technology system.

This project includes both the acquisition of an existing commercial self-scheduling capability and the development of interfaces to integrate that capability with "VA" systems. Development activities will follow the VA processes referenced below.

The Office of Information & Technology (OI&T) has transitioned projects from the Project Management Accountability System (PMAS) project management process into the Veteran-focused Integration Process (VIP) project management process in the 2016-2017 timeframe. VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. VIP is the follow-on framework from PMAS for the development and management of IT projects which will propel the VA with even more rigor toward Veteran-focused delivery of IT capabilities. The VIP framework unifies and streamlines IT delivery oversight and will deliver IT products more efficiently, securely and predictably. 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 a significant evolution from PMAS, creating a more flexible process that has fewer documentation requirements and milestones, and delivers products in shorter timeframes.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
3. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. 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
6. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
7. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
8. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, http://www.va.gov/vapubs/
9. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, http://www.va.gov/vapubs
10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. 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
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
19. VA Handbook 6500.1, “Electronic Media Sanitization,” November 03, 2008
20. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, October, 28, 2015
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
25. OI&T ProPath Process Methodology (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp

26. One-VA Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
29. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
30. VA Directive 6300, Records and Information Management, February 26, 2009
31. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
32. OMB Memorandum, "Transition to IPv6", September 28, 2010
33. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
34. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
35. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
36. 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
37. 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
38. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
39. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
40. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
41. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
42. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
43. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
44. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
45. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
46. 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)
47. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
48. 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)
49. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf

50. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
51. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
52. 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)
53. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
54. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
55. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
59. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
60. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
61. 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
62. 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
63. 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
64. “Veteran Focused Integration Process (VIP) Guide 1.0”, December, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
65. “VIP Release Process Guide”, Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
66. “POLARIS User Guide”, Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412
67. Logical Observation Identifiers Names and Codes (LOINC)
68. Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT).
69. Public Law 114-286, “Faster Care for Veterans Act of 2016”
70. VA Handbook 6517, Risk Management Framework For Cloud Computing Services, dated November 15, 2016

3.0 SCOPE OF WORK

The Contractor shall provide an existing commercially available, off-the-shelf Online Patient Self-scheduling System (OPSS) that includes the minimum capabilities specified in Section 3(a) of PL 114-286 and enables Veterans to use both an Internet website and a mobile application to schedule and confirm medical appointments. The Contractor shall host, install, configure the commercial software, develop the required interfaces to VA scheduling software, and conduct pilot testing of the OPSS in three VISNs for appointments in Primary Care, Specialty Care and

Mental Health. The Contractor shall provide all hosting, software, hardware, training and services necessary to support installation, configuration, integration and piloting of the OPSS capability. The Contractor shall also provide Operations and Maintenance (O&M) supporting the integrated commercial product and interface code throughout the period of performance of this contract.

The Contractor shall follow an Agile Methodology and follow VIP established by OI&T Enterprise Program Management Office (EPMO).

For the purposes of this PWS the tem "Pilot" refers to the fielding and operations of the OPSS described in PWS paragraph 5.5 and all subparagraphs.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) shall be 18 months from date of award with two, 6-month option periods and three optional tasks.

Optional tasks 5.9 for Additional Scrum Team Support and 5.10 for Licenses and Hosting for Installation at Additional Sites may be exercised during the base period as well as both option periods. Optional task 5.11 for Transition can be exercised one time during the last period of performance of this contract.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

There are 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

Tasks under this PWS shall be performed at Contractor facilities.

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 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 related meetings for this effort is four for the base period**.** The Government estimates two to three Contractors for each trip estimated at four days in duration for each VA Medical Center (VAMC) trip and two days for each Washington DC trip; anticipated locations include the following:

1. Minneapolis, MN VAMC
2. Bedford, MA VAMC
3. Salt Lake City, UT VAMC
4. Washington DC

Additional travel will be required if optional task 5.10 for Licenses and Hosting for Additional Sites is exercised. Travel for additional sites is estimated at one trip per site.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform 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 this effort. The CPMP should take the form of both a narrative and Gantt Chart developed utilizing a Technical Reference Model (TRM) approved project management tool detailing the activities required, estimated durations and both Contractor and VA resources required. The project management tool shall calculate such items as the critical path, activities that should have started and those that have not, impacts on project completion, "what if" analysis of issues, cost efficiencies, burn down charts and PowerPoint presentations. The project management tool shall be updated at least weekly and reflect the current project status. All projects tracking data shall be exportable to TRM-approved version of Microsoft Office Project. 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 in accordance with Section B of the contract. The CPMP shall not be re-baselined without the written concurrence of the COR and VA PM. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

The CPMP shall identify the project team organization including project management, scrum masters, and team members. The CPMP shall include the proposed Agile software development methodology. When necessary the CPMP shall include sprint review session formats and responsibilities. Sprints shall not exceed four weeks in duration.

Deliverable:

A. Contractor Project Management Plan

5.1.2 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after contract award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule. The Contractor shall conduct a discussion on alternative approaches to pilot operations by site, by Clinical Service type, in parallel, or sequentially. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the CO, Contract Specialist (CS), COR, and the VA PM.

5.1.3 REPORTING REQUIREMENTS

The Contractor shall use the VA's implementation of the Rational Toolset to provide a single Agile project/product lifecycle management tool to track execution details. The Rational Project/Product Data and Artifact Repository will be used to provide a single authoritative project and product data and artifact repository. All OI&T project data and artifacts will be required to be managed in this data and artifact repository daily. All checked out artifacts shall be checked back in daily and any data updated daily. Rational synchronizes all changed information immediately for all team members to access work proficiently without the concern of working on aged information.

The Contractor shall use VA Rational tools in accordance with the VA Rational Tools Guide to:

1. Input and manage scheduled project/product sprints and backlog
2. Input and manage project/product agile requirements
3. Input and manage project/product risks and issues
4. Input and manage project/product configurations and changes
5. Input and manage project/product test plans and execution
6. Input and manage project/product planning and engineering documentation
7. Input and manage linkages to correlate requirements to change orders to configurable items to risks, impediments, and issues to test cases and test results to show full traceability.

The Contractor shall show all Agile requirements, changes, tests performed and test results in Rational to show evidence of code coverage and test coverage of all the requirements specified. This expectation will allow VA to have high confidence in a fully documented, as evidenced by data in the tools, requirements traceability matrix (RTM).

The Contractor shall provide the COR with Monthly Progress Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month.

The Monthly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also 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 its plan and timeframe for resolving the issue. The report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and its current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. 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.

Deliverable:

A. Monthly Progress Reports

5.1.4 RATIONAL TOOLS TRAINING

The Contractor and Government Project Manager shall determine which team members require access to the Rational Tool Suite. All Contractors that require access shall complete all of the following VA Talent Management System (TMS) training courses within 14 days of the identification of the need for such access.

1. TMS ID 3878248 - IBM Rational Team Concert - Agile Sprint, Configuration/Change Management Level 1
2. TMS ID 3878249 - IBM Rational Team Concert - Agile Sprint, Configuration /Change Management Level 2
3. TMS ID 3878250 - IBM Rational DOORS Next Generation - Requirements Management Level 1
4. TMS ID 3897036 - IBM Rational DOORS Next Generation - Requirements Management Level 2
5. TMS ID 3897034 - IBM Rational Quality Manager - Quality Management Level 1
6. TMS ID 3897035 - IBM Rational Quality Manager - Quality Management Level 2

Contractors who have completed these VA training courses within the past 24 months and have furnished certificates will not be required to re-take the training courses.

Deliverable:

A. Rational Training Certificates

5.1.5 PRIVACY & HIPAA TRAINING

The Contractor shall submit TMS training certificates of completion for VA Privacy and Information Security Awareness and Rules of Behavior and Health Insurance Portability and Accountability Act (HIPAA) training, and provide signed copies of the Contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, "Contract Security".

Deliverables:

A. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificates
B. Signed Contractor Rules of Behavior Certificates
C. VA HIPAA certificates of completion

5.1.6 ONBOARDING

The Contractor shall manage the onboarding of its staff. Onboarding includes steps to obtain a VA network and email account, complete training, initiate background investigations, and gain physical and logical access, which may include elevated privileges to the necessary development and test environments for the various systems to be enhanced.

A single Contractor Onboarding POC shall be designated by the Contractor that tracks the onboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for accurate and timely submission of all required VA onboarding paperwork to the COR. The Contractor shall be responsible for tracking the status of all its staff's onboarding activities and report the status at the staff level during onboarding status meetings. The Contractor shall provide an Onboarding Status Report weekly for any staff with outstanding onboarding requests for review by the COR, VA PM and Project Manager.

Deliverable:

A. Onboarding Status Reports

5.1.7 RISK MANAGEMENT

The Contractor shall conduct risk management of all work performed under this TO and provide input to the product Risk Management registry within Rational.

The Contractor shall:

1. Report, monitor, manage and mitigate risks for each respective product.
2. Enter and update risks in the Risk Log within Rational.
3. Assess the status of its risks on a weekly basis and add them to the risk log within the Rational. When new risks occur which could impact development, testing and deployment schedule, the Contractor shall notify the COR and VA PM via email within 24 hours. Email subject line shall read "{Project Name} Risk Alert Notification."

5.1.8 CONFIGURATION MANAGEMENT

VA will assist the Contractor in creating a Faster Care project within Rational. The Contractor shall be responsible for all day-to-day O&M of the Faster Care project within Rational including check-ins, check-outs, and builds. The Contractor shall:

1. Identify the standard and unique aspects of configuration management to be performed for each project by establishing a Configuration Management (CM) Plan which meets EPMO CM plan requirements. The Contractor shall reflect all CM required activities and standards in each project-level CM plan while determining the unique aspects of the project which require individualized procedures.
2. Deliver a List of Configuration Items to be placed under configuration and change control, which shall be documented in the Configuration Management Plan. The Contractor shall identify types of configuration items pertaining to each product to be placed under configuration management. Based on EPMO requirements, and the unique needs or nature of each project, the Contractor shall determine the components within each project that must be under configuration control.
3. Use Rational Team Concert as the VA approved tool and repository for all software source code and electronic artifact configuration and version management. The Contractor shall use the Rational Team Concert tool to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes.
4. Ensure that all project software and non-software artifacts are versioned correctly and follow a build/release promotion versioning approach which identifies all major, minor, and updated changes to the components.
5. Create Project and Product Artifacts baselined and versioned in the Rational CM repository in order to allow the tool to show active and past histories of the check-ins and

check-outs of all software components, data, and software product engineering documents. Maintain all baselines of software, software builds, and electronic artifacts in the repository, labeling updates and versions according to CM procedures.

6. Develop, verify and submit with all project build deliveries, a Version Description Document that conforms to EPMO Website standard templates and addresses the manifest of the contents of all software builds created for project releases outside the development environment.
7. Establish and maintain status reporting on change and configuration management activity, and ensure Rational Team Concert data records and artifacts are filed and updated daily.

Deliverables:

A. Configuration Management Plan
B. Version Description Document

5.2 VIP DEVELOPMENT LIFECYCLE

The Contractor shall follow the VIP development lifecycle for all development work done in support of OPSS.

Agile project management is evolutionary (iterative and incremental) which regularly produces high quality results in a cost effective, timely, and highly collaborative manner via VIP's value driven lifecycle. This requires open lines of communication among all participants contributing to a project/program/portfolio that include multiple consumers within the contracts and with other VA offices/activities.

VIP describes a schedule of incremental deliveries of useable capabilities every three months or less.

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance. Based on the scope of work established in the Backlog, development builds shall be three months or less.

The foundational structure for VA agile development and project management can be found in the VIP Guide. For delivery of all project artifacts, the Contractor shall utilize Rational for managing project execution details and for the management and storage of artifacts using approved VIP and/or EPMO website templates.

The Contractor shall provide a Certified Scrum Master and a scrum team to follow the Agile methodology as described below and in the VIP guidelines. The scrum team for this effort shall be composed of an evolving mix of technical skill sets as required to meet the necessary stage of the software development lifecycle and technical nature of the project. The Contractor shall adjust deliverables and technical Rational updates to match the nature of the software development.

The Contractor shall provide a scrum team (VA estimates approximately 11 to 12 Full Time Equivalents (FTE)) with the appropriate technical skill sets to support installation and configuration requirements in PWS section 5.3, the VA interface development required in PWS section 5.4, and the pilot project operation and evaluation support required in PWS section 5.5. This scrum team shall support PWS tasks 5.3 through 5.5 in the base period, and continue

support of pilot operations described in PWS task 5.5 in the option periods (if exercised) of this contract.

5.2.1 AGILE REQUIREMENTS ELABORATION

The Contractor shall complete an initial backlog grooming session with the COR/VA PM team to properly review and elaborate business Agile requirements. The outcome of this session shall be a complete review of, and agreement to, the initial user stories, including user stories added as a result of backlog grooming by decomposing epics into stakeholder needs, business requirements, business rules, requirements visualizations, and user story elaborations.
The Contractor shall:

1. Ensure all requirements as defined in PWS paragraph 5.3 through 5.5 are included and executed as appropriate within the overall Agile backlog grooming effort.
2. Evaluate the Project backlog during an initial planning session to identify all features the team considers relevant to building the product. The backlog serves as the primary source for all project requirements and user stories.
3. Establish initial Unit of measurement (e.g. Story Points) as the estimated relative complexity of user stories.
4. Facilitate any stakeholder briefings, meetings, and/or requirements elicitation sessions.
5. Execute requirements reviews with stakeholders and record results of reviews for the project-specific requirements identified in PWS paragraph 5.3 through 5.5 using Rational, updating requirements data as a result of the reviews.
6. Identify the development and test environment access that is needed 30 days prior to development start.
7. Input and maintain all Epics, stakeholder needs, visualizations, stories, and other sources of requirements information for functional and non-functional requirements in Rational. All requirements data is under change control and is fully linked to work items that show traceability to design changes, configurable items, test cases, and test results.

5.2.2 BUILD AND DEVELOPMENT

The Contractor shall continuously support the iterative build and development methodology described below in order to complete all epics and user stories identified in the backlog.

5.2.2.1 SYSTEM DESIGN DOCUMENT

The Contractor shall update and maintain the System Design Document (SDD) for each build, updating at the end of each sprint, as necessary. The Contractor shall ensure that the detailed design includes the development of detailed data and process models, screen and report designs, interface specifications and control specifications.

The SDD shall include the following:

a) Detailed` system/solution architecture to include system schematics, system and subsystem performance-based descriptions, and key interfaces between the system and subsystems
b) Hardware and software specifications to include sizing and performance requirements, systems and subsystem interface requirements, and systems control requirements
c) Standards utilized
d) Security Controls
e) Enterprise services utilized
f) Database and file structures
g) Data flows, data dictionary entries, and lists of inputs/outputs by subsystem

h) Special design considerations (e.g., network design approaches)
i) Capacity, performance and business continuity requirements
j) Utilize organizationally established architecture tools, repositories, and repository management processes to capture, publish, and maintain architecture artifacts
k) Solution design documents and artifacts necessary to provide ongoing sustainment support

System Architecture Diagrams shall be updated during all build cycles and incorporated into the SDD as required.

Deliverable:

A. System Design Document and updates

5.2.2.2 BUILD PLANNING

The Contractor shall develop a Build Plan in Rational prior to the start of each build. Each build shall be no longer than three months in duration and shall be made up of individual sprints that are not to exceed four weeks in duration. Each build will be fully tested by the Contractor and by a VA test team, and will end in a new release candidate. The Contractor shall continuously maintain the Project Backlog for each build, in every release and throughout the life of the period of performance within Rational. All activity scheduled in each build and backlog will be captured and have status showing all work items, changes, impediments, and retrospectives. All data and artifacts in the Rational shall be fully linked to requirements data and test data.

The Contractor shall perform the following during build planning which is in coordination with the COR/VA PM and the VA project teams:

1. Review, elaborate, and prioritize the project backlog. This backlog grooming will occur continuously throughout the build to ensure the customer's highest priorities are being met.
2. Specify all Key Performance Indicators (KPI)
3. Facilitate project backlog grooming and Build Planning sessions that outline the intent of the build. The Contractor shall update the resulting Build Plan within the Rational.
4. Identify the epics and user stories to be completed within the build, the agreement of acceptance criteria of the build, and readiness to begin build.
5. Conduct additional requirements elaboration to the extent necessary to break the epics into user stories in order to develop a Build Plan and maintain the backlog. Teams will review, elaborate, and prioritize the backlog. This backlog grooming will occur continuously throughout the build to ensure the customer's highest priorities are being met.
6. Joint determination of the Definition of Done for the features within the build.
7. Conduct backlog prioritization meetings with OI&T and VA Business representation with results updated into backlog.

The Build Plan shall include:

1. High-level Epic
2. Feature Breakout
3. Relationship Traceability
4. Key Performance Indicators
5. Success Criteria

6. Identified Dependencies (internal and external)
7. Approved wireframes (if needed)
8. Functional Design
9. Technical Approach
10. Definition of Done

Deliverable:

A. Build Plans
B. Project Backlogs

5.2.2.3 SPRINT PLANNING

Once the build plan is completed, reviewed and approved by the COR/VA PM, the Contractor shall initiate Sprint Planning for the first Sprint of the build. All activity scheduled in each sprint and backlog will be captured and have status showing all work items, changes, impediments, and retrospectives in Rational. All data and artifacts in Rational shall be fully linked to requirements data and test data.

The Contractor shall:

1. Initiate and participate in a Sprint Planning Meeting, at the beginning of each sprint. The Contractor shall update the Sprint Plan in Rational at the conclusion of the Sprint Planning.
2. Support, coordinate and provide input for the Sprint Acceptance Criteria in Rational The Sprint Acceptance Criteria shall be coordinated and approved by the COR/VA PM for every sprint.

Deliverable:

A. Sprint Plan

5.2.2.4 SPRINT EXECUTION

All activity executed in each sprint and backlog will be captured and have status showing all work items, changes, risks, issues, impediments, and retrospectives in Rational. All data and artifacts in Rational shall be fully linked to requirements data and test data. All project artifacts and source code will be under change and configuration management as specified by the COR using Rational.

The Contractor shall:

1. Provide a certified Scrum Master to facilitate all ceremonies, ensure Rational is updated daily, enforce scrum framework, and track and assist with removing impediments.
2. Develop the features and capabilities as work items in Rational that were established in the Sprint Plan.
3. Complete sprint development including disciplined testing (unit, functional, regression) and reviews as a continuous process, to avoid finding issues at the end of sprint development.
4. Initiate and conduct daily scrums (typically 15 minutes) to show the team progress, impediments, and daily plans.
5. Update Rational daily, to include progress on tasks during sprints, to include issues, and dependencies.

6. Coordinate and support demonstration of the sprint activities in a Sprint Review with the VA project team and users at the end of each sprint to obtain customer acceptance of the sprint in collaboration with the COR/VA PM.
7. Initiate and facilitate a Sprint Retrospective at the end of the Sprint to capture performance lessons learned.
8. Deliver Source Code in Rational.

The Contractor shall ensure that content developed for OPSS is expressed in nationally recognized reference and authoritative terminology standards such as, Logical Observation Identifiers Names and Codes (LOINC), and Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT). Where data is required to be entered to OPSS, the Contractor shall require data entry using standardized terms.

Any code developed under this PWS will be released to the open source community with all VA-sensitive information redacted. Since the VA-sensitive information redaction process is required, the Contractor shall develop code in a compartmentalized manner to facilitate redaction activities and maximize the functionality of the redacted code. Coding which is not correctly designed for VA-sensitive information redaction and submission to the open source community shall be considered to be incomplete and require revision by the Contractor. Code to be submitted to the open source community shall be licensed by the Contractor under the Apache License, Version 2.0 (http://www.apache.org/licenses/LICENSE-2.0.html).

Deliverable:

A. Source Code and Rational Updates

5.2.2.5 TESTING

The Contractor shall adopt Agile best practices for testing into each Agile development sprint and build. The Contractor shall populate the Test Strategy Data section of the test plan in Rational 10 days prior to the first sprint for each build. The Contractor shall conduct tests as applicable (e.g. including unit, functional, accessibility, Section 508, user acceptance, system, reliability, usability, interoperability, regression, security, penetration, performance, end to end) throughout the development lifecycle (e.g. user story, sprint, build, release). The Contractor shall perform Regression/ Software Quality Assurance Testing (SQA) in collaboration with the PM/COR appointed VA SQA tester(s) prior to releasing software code into pre-production and production environments. The Contractor shall apply industry best practices of continuous integration methods and automated regression testing utilities using One-VA TRM approved tools. The Contractor shall conduct testing related to non-functional requirements, including load, performance, installation, back-out, and rollback.

The Contractor shall provide Test Plan data in the Rational Quality manager, following the templates and data requirements appropriate for each sprint. The Contractor shall provide test results in the Rational Quality Manager, which is the final piece of data that completes the RTM. COR/VA PM approval will occur through the rational Quality Manager approval process. The Contractor shall support both Compliance Reviews and Verification and Validation testing activities in accordance with the VIP. The Contractor shall assist in the compilation of data for VA submission and respond to requests for changes to code or documentation resulting from those reviews, as necessary.

The Contractor shall support the security, accessibility, performance, technical standards, architectural compliance, user acceptance, and initial operational capability tests, audits, and reviews. The Contractor shall perform security scanning multiple times throughout the course of a project using Fortify. The Contractor shall request infiltration (Web Application Security Assessment (WASA) / Mobile Application Security Assessment (MASA)) testing from the VA Network and Security Operations Center (NSOC) for all major builds prior to deployment to the production environment. The Contractor shall conduct performance testing through load testing and technical analysis of capacity planning data submitted by the project team. Architectural compliance assessments are done by VA through submission of design materials to confirm compliance with allowed enterprise architecture; the Contractor shall support documentation revisions required resulting from this review.

The Contractor shall ensure all test and compliance review planning and execution details and its testing and compliance results are entered, maintained and under version control in the Rational Quality Manager. Specifically test management data and artifacts include such items as scripts, configurations, utilities, tools, plans, and results. The Contractor shall ensure that results of all assessments of the project performed by the Contractor or by VA offices are consolidated into Rational for planning and status reporting. The Contractor shall provide the following testing documentation:

1. Test Plan
2. Test Execution Data
3. Test Results
4. Defect Logs

When a defect is identified during testing, the Contractor shall log it in Rational, selecting the appropriate severity level. The Contractor shall support the COR/VA PM in prioritizing the defect in the sprint backlog. Based on priority, the defect may be entered into the current sprint or entered into the backlog.

The Contractor shall maintain traceability from the requirements to test cases, test execution, test results and defect logs in Rational. The Contractor shall ensure rational data is up-to-date on a daily basis so that VA stakeholders can access accurate and timely status.
The Contractor shall provide OPSS system access, demonstration and technical information as required in support of external validation and verification requirements mandated by PL 114-286.

Deliverables:

A. Test Strategy Data
B. Test Plan
C. Test Scripts
D. Test Execution Data
E. Test Results and Defect Logs

5.2.2.6 BUILD DELIVERY

The Contractor shall provide a Build Acceptance Form when each build is acceptable for VA release and all deliverables required for that release are current and resident in Rational. This includes all documentation, source code, and test results to be delivered, resolved and approved by VA COR. The Build Acceptance Form shall also be provided by the Contractor for

acceptance for Pilot Operations support in accordance with PWS Task 5.5, Pilot Project Operation and Evaluation Support.

Deliverable:

A. Build Acceptance Form (Contractor Format)

5.3 OPSS START-UP AND CONFIGURATION

The Contractor shall provide the hosted existing commercially available, off-the-shelf OPSS capable of interfacing with the existing VA scheduling software and supporting systems. The OPSS shall provide the ability for Veterans to use an Internet website and mobile application to schedule and confirm medical appointments at VA medical facilities. The solution shall provide the capability to run on the operating system of a cellular telephone, tablet computer, or similar portable computing device that transmits data over a wireless connection. All applications shall be designed to operate within iOS, Android, and Windows, and wrapped in PhoneGap or similar technology for native installation.

The Contractor shall complete the Section 508 Self-Certification Document. The Contractor shall support the VA Project Manager in obtaining the 508 compliance testing certifications for the OPSS. Specific documents and information to be used to implement policies from the Section 508 Rehabilitation Act of 1973 and VA's Section 508 Accessibility Mandate can be found at http://www.section508.va.gov/.

The Contractor shall provide an Online Patient Self-Scheduling COTS solution capable of meeting the following congressionally mandated scheduling requirements:

1. Capabilities to schedule, modify, and cancel appointments for primary care, specialty care, and mental health.
2. Capability to support appointments for the provision of health care regardless of whether such care is provided in person or through telehealth services.
3. Capability to view appointment availability in real time.
4. Capability to make available, in real time, appointments that were previously filled but later cancelled by other patients.
5. Capability to provide prompts or reminders to Veterans to schedule follow-up appointments.
6. Capability to be used 24 hours per day, 7 days per week (meeting VA 99.99% availability requirement)
7. Capability to integrate with the Veterans Health Information Systems and Technology Architecture (VistA) of the Department, or such successor information technology system.

In order to meet these Congressionally mandated requirements identified in PWS paragraph 1.0, Background, and at Section 3(a) of PL 114-286, the solution shall support current VA scheduling processes with the following capabilities:

1. Capable of accessing a calendar / list of available appointments for the authenticated Veteran to book in real time from specific VA facilities based upon
    a. Veteran identity,
    b. Veteran relationship to facility
    c. Capable of reading a Veteran's past appointment history at the facility

    d. Facility-established settings for Veteran direct booking/cancellation of appointments
2. Capable of restricting the booking of appointments to clinics designated as allowing direct booking in the VistA scheduling package.
3. Capable of determining that the Veteran is enrolled in VA healthcare and is registered with a VA facility.
4. Capable of determining and displaying only available clinical services particular to each pilot site
5. Capable of displaying to the Veteran his/her currently booked appointments at a facility based upon real-time data with the display showing the name of the clinic, the Veteran-friendly clinic name, the date, and time of the appointment.
6. Capable of real-time display of appointment availability, with ability to resolve conflicts and prevent duplicated appointments in an environment where multiple systems may be interacting with VistA, the authoritative scheduling package. Current systems that interact with VistA and can book appointments are the Veteran Scheduling Enhancement App, Schedule Manager App, Veteran Appointment Request App, and VistA Scheduling.
7. Capable of capturing the Veteran's preferred date when booking or cancelling an appointment at the beginning of the process.
8. Capable of capturing all information required to book or cancel an appointment in VistA
9. Capable of limiting the scheduling of Primary Care and Mental Health appointments to providers for whom the patient has an existing relationship. Specifically, Primary Care appointments will be scheduled with the Veterans Patient-Aligned Care Team (PACT) using data from the Primary Care Management Module (PCMM) to validate the Primary Care Team relationship. For Mental Health and Specialty Care, the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months.
10. Capable of providing the Veteran with prompts to schedule follow-up appointments based upon VA provided business rules
11. Capable of providing Veterans with the ability to complete and submit a Right of Access (ROA) form in order to access their information from VA. The Contractor shall retain ROAs throughout the PoP and transition them to VA at the conclusion of the contract.
12. Capable of verifying that a signed ROA form has been completed prior to the Veteran accessing data in the future.
13. Capable of providing VA access to all ROA forms.
14. Capable of providing the Veteran an End User License Agreement (EULA) with text approved by VA.
15. Veteran shall only be able to use the app if they have agreed to the EULA.
    a. Veteran must be able to view a copy of the EULA while using the app.

5.4 VA SYSTEM INTEGRATION AND INTERFACE DEVELOPMENT

Prior to pilot testing, the Contractor shall develop, test and implement the VA interfaces to implement the requirement described at Section 3(a)(7) of PL 114-286: Capability to integrate with the Veterans Health Information Systems and Technology Architecture of the Department.

For each pilot site and Clinical Service type, the Contractor shall develop, test and support installation of the required interfaces between OPSS, VistA and other VA systems required to enable pilot testing of the minimal required scheduling capabilities identified in PWS section 5.3. The Contractor shall identify and develop all required interface requirements following the VIP Development Lifecycle defined in PWS task 5.2, and submit them for VA approval.

The following requirements apply to enable interaction with VA scheduling and other supporting systems. The Contractor shall be responsible for providing all hardware, software, licensing, operation and maintenance components required for successful hosting and operation of the OPSS and interfaces.

OPSS integration with VA systems requires:

1. Hosting within a FISMA High, TIC 2.0 compliant environment with 99.99 percent availability.
2. Capable of integrating with an existing Veteran authentication method that integrates with VA's Identity and Access Management System (IAM) such as DS Logon.
3. Network connectivity that complies with FIPS 140-2, Section 1, Table 1, up to and including Security Level 3.
4. A redundant, secure encrypted network solution providing connectivity to the solution and secure connectivity to VA systems.
5. A Business Partner Extranet (BPE) to connect to the VA network. The Contractor shall document, justify, and submit BPE configuration change requests to the Enterprise Security Change Control Board (ESCCB) for approval as required.
6. Capable of validating that the user is registered in the VA's VistA system through the IAM integration. This includes integration with the Master Veteran Index (MVI). MVI will provide the OPSS system with the VistA sites where the Veteran is registered for healthcare as well as provide the unique identifiers (such as the Integration Control Number (ICN)) for the Veteran.
7. Capable of accessing patient data from multiple VistA systems based upon the Veteran unique identifier/ICN.
8. Capable of providing non-authenticated users a statement that they must be registered for care with VA while providing resources describing eligibility and enrollment information.
9. HIPAA compliant.
10. Section 508 compliant
11. Capable of maintaining logs of all access of patient data and all read/write activity to VistA. Patient access logs need to be maintained through the PoP and transitioned to VA at the conclusion of the contract.
12. Capable of logging all individuals who access a Veteran's data stored in any way within the OPSS system
13. Capable of integrating with VistA using VA provided middleware/application programming interfaces, ~~VA-approved web services,~~ remote procedure calls (RPC), and security standards, etc.
14. Capable of becoming VA TRM approved.

5.5 PILOT PROJECT OPERATION AND EVALUATION SUPPORT

The Contractor shall provide the hosting, licenses/Software as a Service (SaaS) as applicable to the commercial product proposed. The Contractor shall conduct pilot operations demonstrating OPSS capabilities to directly schedule and confirm appointments at one VA facility located in each of three different VAMCs: Minneapolis, MN, Bedford, MA, and Salt Lake City, UT. Provider participants in the pilot are estimated as follows:

	Primary Care	Specialty Care	Mental Health	Total
Bedford, MA	9	52	40	101
Minneapolis, MN	35	70	61	166
Salt Lake City, UT	25	52	40	117

~~at 250 from Minneapolis, 150 from Bedford, and 250 from the Salt Lake City VAMCs.~~ These appointments shall be scheduled in Primary Care, Specialty Care (e.g. Audiology and Optometry), and Mental Health Care at each of the sites. Clinics will be designated for participation in the pilot using currently existing flags in the VistA clinic profile that will "turn on" the clinic to the internet web site/mobile application scheduling solution. The user base for the pilot test shall include every patient who has had an appointment at the pilot site within the last 13 months in Mental Health or Specialty Care or are assigned a Primary Care Provider. The pilot shall process at a minimum 100 successful direct scheduling events during each month at each pilot facility distributed across Primary, Specialty and Mental Health care with at least some appointments scheduled in each clinical service area (Primary, Specialty and Mental Health).

5.5.1 AUTHORITY TO OPERATE

The Contractor shall provide all Assessment and Authorization (A&A) support required to achieve and maintain full A&A certification in compliance with the most current versions of VA Handbook 6500, VA Handbook 6500.6 (Section 3), and VA Handbook 6500.3. The A&A process is the end to end process for ensuring new VA information systems adhere to and are in compliance with FISMA. The purpose of an Authority to Operate (ATO) is to ensure the risks to VA (operations, assets, or individuals) are acceptable. The result is the issuance of an ATO. If the risk to Agency operations, assets or individuals is low, an ATO authorizes the system to be moved into production or use production data. The Contractor shall develop and submit all required security document artifacts as described in ProPath (http://vaww.oed.wss.va.gov/process/maps/process_AAA.pdf).

VA requires an ATO for both the OPSS and the external hosting environment. After ATOs are achieved, the Contractor shall update and maintain the ATO documentation as required to ensure compliance.

An ATO is required for the project to achieve a Critical Decision 2 (CD2) approval to enter the Pilot phase.

Also in addition to the NIST 800-53 Rev 4 controls, the Contractor shall:

a) Perform bi-weekly reviews of Plan of Actions and Milestones (POA&M) with the VA PM/COR to ensure backlog is scheduled and prioritized for remediation, and to verify that defined milestones will be achieved.
b) Perform monthly reviews of Risk Based Decisions with the VA PM/COR to ensure remediation to outstanding risks or path forward is identified and achievable.
c) Support documentation of a Data Use and Reciprocal Support Agreement (DURSA)/Memorandum of Understanding (MOU) / Interconnection Support Agreement (ISA) between the cloud hosting environment and VA

Deliverable:

A. A&A Package for the OPSS
B. A&A Package for the OPSS Cloud Hosting Facility

5.5.2 PILOT PLANNING

The Contractor shall develop a Pilot Strategy and Plan Document for COR review. The Document shall detail the timeline, tasks, and VA involvement required for conducting the pilot program. The Contractor shall include details on their approach including its rationale for conducting the pilots at three sites simultaneously, sequentially, by Clinical Service type, or other. The Contractor shall review the Document with the VA PM/COR and revise as required. It is important to note that a VIP CD2 approval will be required before this project goes into its Pilot phase. The Contractor shall communicate with the VA workforce and conduct onsite training at each pilot site (estimated at one session per site). The Contractor shall coordinate with VA to identify, notify and educate patient pilot participants at each site.

Deliverable:

A. Pilot Strategy and Plan Document

5.5.3 END USER TRAINING MATERIALS

The Contractor shall provide commercially available training materials to assist with the training of end users of the system. Training materials may include the following: Word Documents, PDF Documents, Presentations, Wiki Pages, Audio Clips, or Videos. The Contractor shall provide training materials and a knowledge base that will be accessible through the application. The Contractor shall ensure all end user functionality in the system is accounted for in training materials and knowledge base.

The Contractor shall:

1. Provide end user Training Materials
2. Provide, implement and manage an online Knowledge Base Repository

Deliverables:

A. Training Materials
B. Knowledge Base Repository

5.5.4 PILOT OPERATION

Prior to CD2, the Contractor shall ensure that all required documentation is assembled and up to date including:

1. Requirements: This section should cover business, functional, non-functional, technical and all other requirements included within the Epics, Sub-Epics and User Stories. The Release agent will be verifying that the documentation is current and approved.
2. Traceability: Traceability, Test Execution, Test Results, defect log. Verification that release Epics and User Stories are covered in a sprint Plan and there are subsequent test results, including acceptance criteria.
3. Risk: Risk Log report. The VA Release agent will examine the risk log in the Data Repository for the status and the exposure of given threats.

Additionally, the Contractor shall:

a) Develop the Production Operations Manual (POM) incorporating the Deployment, Installation, Back -Out, Rollback Plan, Responsible/Accountable/Consulted/Informed (RACI) (If extensive deviations required), Troubleshooting Information, Process

Flowcharts and Key Monitoring Indicators which are all subsections within the POM document.

b) Develop /update the Technical Manual for VA Interfaces
c) Develop/update the User Manual
d) Develop/update the Version Description Document.

During pilot release, the POLARIS calendaring process and tool will be used to track software installations, hardware replacements, system upgrades, patch release and implementation, special works in progress, and other release events in the VA production environment. The Contractor shall provide data for populating and updating the POLARIS calendaring process for each release and deployment.

Upon obtaining a project CD2 approval, the Contractor shall initiate pilot operations at the three test sites.

The Contractor shall provide OPSS licenses and hosting sufficient for pilot operations. The Contractor shall conduct the Pilot project and provide evaluation support by performing the following activities and complying with VA standards and procedures:

a. Coordinating pilot activities with VA and pilot participants and:
    1) Coordinate and conduct meetings with all stakeholders (i.e., Strategic Technology Alignment Team (STAT), Design, Engineering and Architecture (DEA), Release management, Health Product Support and 508 Program Office to obtain approvals and support for pilot evaluation from all concerned parties. The Contractor shall inform the COR/VA PM of the results of Pilot entry initiation.
    2) Identify any site-specific policies and procedures as well as identifying site-specific environment preparation requirements
    3) Validate field sites, test environments, acceptance criteria, and ATO requirements.
    4) Coordinate and validate MOUs, ISAs and Service Level Agreements (SLA) for partner dependencies that specifically highlight the commitment of partners to associated release.
    5) Continue communication with the VA workforce.
    6) Continue coordination with VA to identify, notify and educate patient pilot participants at each site
    7) Distribute access to the OPSS system and documentation at each site
    8) Provide timely installations at the each site
    9) Set up and conduct formal, bi-weekly Evaluation Site calls
    10) Configure the OPSS system for operation at each site
    11) Install and test the OPSS interfaces at each site as required.

b. Establishing and monitoring scheduling performance metrics to monitor pilot success.
c. Drafting and/or assembling OPSS system installation request and any required artifacts no later than 15 days prior to initiation of the Pilot Project at a specific site. It shall be noted that the required artifacts may change over time as the VIP process matures.
d. Tracking defects identified during Pilot Evaluation, and as per direction from the VA PM will remediate defects found during the Pilot Evaluation. Upon remediation, the Contractor shall provide to all Pilot sites the updated/remediated solution for testing and acceptance.

e. Support verification testing, addressing issues and questions regarding the OPSS system identified during implementation and evaluation
f. Deliver Final Source and Executable Code reflecting any updates resulting from pilot operations.
g. Provide VA use metrics based upon times on the number of unique users, number of booking attempts, number of cancellation attempts

Deliverables:

A. Updated Production Operations Manual
B. Updated Technical Manual
C. Updated User Manual
D. Updated Version Description Document
E. OPSS Licenses and Hosting
F. Final Source and Executable Code

5.5.5 PILOT ANALYSIS

The Contractor shall conduct an evaluation of the pilot test and document the findings in a Pilot Test Evaluation Report. The Contractor shall document any results obtained, any issues encountered, pilot user feedback, and lessons learned. The report shall provide clear explanations of how critical design features of the system performed and lay out a comprehensive advanced development and integration plan for subsequent development, scaling and integration into VA IT systems. The report shall include summary statistics on pilot operations including:

1. Veteran Experience: Veteran survey of a select cohort of users who used or attempted to use the OPSS, assessing
    a) Satisfaction with the overall experience (1-10, with comments)
    b) Ease of use of the OPSS (1-10, with comments).
    c) Convenience of using the OPSS for self-scheduling (1-10, with comments)
    d) "Would you recommend this OPSS to a fellow Veteran?" (1-10)

2. OPSS Functionality
    a) Number of users who logged into the OPSS.
    b) Number of successful scheduling events
    c) Number of unsuccessful scheduling events
    d) Number of appointments cancelled.
    e) Number of scheduled appointments kept.

3. Impact of OPSS on staff : Survey of selected cohort of clinical staff, assessing
    a) Overall satisfaction with the self-scheduling OPSS.
    b) Level of added effort required to support self-scheduling workflow changes, driven by the OPSS.
    c) Scheduler time spent supporting, monitoring, or configuring the OPSS

4. Technical System Performance
    a) OPSS latency
    b) OPSS response time
    c) System up-time

d) OPSS load capacity.

At the conclusion of the Pilot project, the Contractor shall Document the Pilot Exit Review and acquire all required signatures on the exit documentation no later than five days after completion. Required signatures may include:

a) Business Customer Representative
b) Business Owner Representative
c) Enterprise Systems Engineering (ESE)
d) Release Office Representative
e) Head of Enterprise Program Management Office (EPMO) or designee
f) Head of Product Support or Designee
g) Head of Service Delivery and Engineering (SD&E) or designee
h) Other Stakeholders (as necessary)
i) Security Office Representative

Deliverable:

A. Pilot Test Evaluation Report
B. Pilot Exit Review

5.5.6 RELEASE TO OPEN SOURCE

All code developed to meet the requirements of this PWS will be made available to VA's open source community.

As a result, the Contractor shall create an Open Source Submission Package per OPSS for COR/VA PM submission to the open source code repository for certification. This package shall include:

a) All developed source code to be submitted.
b) Automated tests and test data as required by the code repository.
c) M-Code Primary Developers checklist (for M-code only).
d) Technical articles describing the functional goals of the code, the use of the code and any additional details that may help a user of the package or subsequent developers who may maintain the package. Technical articles shall follow the style of a technical report, with particular focus on providing guidance for future use and maintenance of the code contributed to the open source community.

Deliverables:

A. Open Source Submission Packages

5.6 HELP DESK SUPPORT

During pilot operation, the help desk shall provide existing help desk support for the commercial scheduling project throughout the pilot testing period. The Contractor shall interface with the VA Health Resource Center or National Service Desk as required to provide a seamless interface to all Veteran-facing questions. The Contractor shall assist OPSS pilot support staff and participants with questions relating to the use of OPSS to include training support, and responding to basic functional questions that do not involve system errors or bugs. The Contractor shall address user problems directly related to the OPSS software installation and forward bug fixes to the pilot support team. Help desk activities in support of OPSS shall be included in the Monthly Progress Report.

5.7 OPSS OPERATIONS AND MAINTENANCE

The Contractor shall:

a) Create an O&M Plan. The updated O&M Plan shall include the Contractor's concepts, methods and resources that shall be utilized to provide the required O&M support for OPSS as described in the tasks below.
b) Perform OPSS O&M activities identified below in accordance with the approved O&M Plan.
c) Provide a summary of monthly O&M activities from each subtask below and key operating statistics as part of the Monthly Progress Report.

Deliverable:

A. O&M Plan

5.7.1 APPLICATION ADMINISTRATION

The Contractor shall ensure that OPSS renewals, version upgrades, and Commercial Off-The-Shelf (COTS) patches/upgrades are implemented as required. The Contractor shall renew the maintenance agreements annually on behalf of VA. Additionally, the Contractor shall present version upgrades with an assessment of implementation risk to the COR to determine if upgrade contents are applicable to VA and can be installed without issue. The Contractor shall estimate the impact of upgrades to customized code to ensure the scope of the upgrade implementation on OPSS is fully defined. The Contractor shall implement version updates upon COR approval. The Contractor shall provide ongoing application administration support including:

a) Establish Backup Schedules
b) Establish Monitoring Requirements and Parameters
c) Implement Software Upgrades
d) Configure and Install Software patches / version updates, Scripts and Parameter Settings
e) Tune OPSS to resolve application performance issues
f) Monitor Application Logs
g) Data Retention – the Contractor shall ensure that OPSS data is retained, accessible and editable throughout the period of performance of the contract.

5.7.2 PERFORMANCE MANAGEMENT

The Contractor shall provide ongoing performance management support by ensuring that the uptime requirements of the system are met, monitoring services, and proactively responding to projected system demands. The Contractor shall:

a) Develop and maintain OPSS Performance Management Plan
b) Collect system statistics and monitor system availability to ensure OPSS meets availability requirements of 99.99 percent.
c) Collect Help Desk Metrics – Calls answered, issue or problem resolved and compliance with current COTS SLAs.
d) Isolate performance issues to the application and/or the hosting environment
    1. Develop and Implement availability and performance improvements to meet pilot requirements.
    2. Monitor Application Software Performance
    3. Monitor Database Server Performance
    4. Monitor Hardware Performance
    5. Monitor Hosting Network Performance
    6. Monitor Operating System Performance

Deliverable:

A. Performance Management Plan

5.7.3 BUSINESS (SERVICE) CONTINUITY MANAGEMENT

The Contractor shall provide ongoing Business (Service) Continuity Management encompassing Disaster Recovery (DR) and Continuity of Operations (COOP) planning and support. The purpose of Business (Service) Continuity Management is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required and agreed-upon business timeframes. The Contractor shall:

a) Maintain the COOP/DR Plan
b) Create and maintain the COOP/DR Testing Schedule
c) Perform OPSS Recovery Test at the DR/COOP site

Deliverable:

A. COOP/DR Plan

5.7.4 INCIDENT MANAGEMENT

The Contractor shall coordinate appropriate resources to address incidents (e.g. functional errors, availability/uptime, accessibility and security incidents) and communicate incident related information for situational awareness within two hours of the incident to the COR and VA PM. The Contractor shall:

a) Document Incident Escalation Procedures
b) Escalate Incidents/Requests
c) Issue Incident Response Messages (IRMM) and/or Activity Not Responding (ANR) Messages for Critical Maintenance
d) Log and Track Incidents/Requests
e) Notify COR of Incident
f) Perform Triage for Incidents/Requests
g) Provide Incident Reporting and Distribution
h) Respond to Incidents/Requests
i) Identify hosting or application changes required to ensure similar incidents will not occur.
j) Implement hosting or application changes upon approval of the COR.

5.7.5 NETWORK ADMINISTRATION

The Contractor shall implement and maintain the communications infrastructure utilized by OPSS. Network administration responsibilities include the hosting environment network and network communications through the TIC and the interfaces to VistA. The Contractor shall:

a) Manage network connectivity.
b) Monitor network and identify issues as they occur.
c) Process updates as required for network changes and connectivity issues.

5.7.6 SECURITY MANAGEMENT

The Contractor shall protect information from harm due to failures of confidentiality, integrity and availability; meet security requirements of the business; and provide a basic level of security (security baseline). The Contractor shall:

a) Perform recurring security activities required to ensure that OPSS and hosting environments remain in compliance with VA / ATO security requirements.
b) Maintain Interconnection Security Agreements (ISAs)
    1. Maintain Privacy Impact Assessment (PIA)
    2. Maintain Risk Assessment
    3. Maintain Security Configuration Checklists
    4. Maintain Security Plan
    5. Ensure Firewall Security
    6. Ensure Physical Security of Facility
    7. Generate Reviews and Audit Reports
    8. Manage and Review Application Access Logs
    9. Perform Security Audits
    10. Perform Security Controls Testing
    11. Validate Application Security Measures
    12. Perform Vulnerability Scanning

5.7.7 SYSTEM ADMINISTRATION

The Contractor shall perform the processes related to hardware and operating systems, particularly changes to configuration that are released to the environment. The Contractor shall:

a) Update System Administration Guide for changes as required
b) Create User Authorizations and Profiles
    1. Notify the COR of Scheduled System Outages/Preventative Maintenance
    2. Ensure Power Monitoring (Uninterrupted Power Supply (UPS) and Generator)
    3. Monitor and Maintain System Logs
    4. Perform File Transfers
    5. Process backups

5.8 OPTION PERIODS

There are two six-month option periods in the event that VA extends the duration of the pilot program. The Contractor shall perform tasks described in PWS sections 5.1, 5.5, 5.6 and 5.7 required to continue pilot operations established in the base period including renewal of licensing and hosting agreements as required. Optional tasks 5.9, 5.10 or 5.11 may be exercised in either option period.

5.9 ADDITIONAL SCRUM TEAM SUPPORT – OPTIONAL TASK

Throughout the PoP, VA may require additional scrum team support for implementation of OPSS at additional sites, additional configuration, or implementation of additional functionality that was not included in the initial pilot implementations. The Contractor shall provide additional, smaller scrum teams (VA estimates approximately five to six Full Time Equivalents (FTE)) with the appropriate technical skill sets to support installation and configuration requirements in PWS section 5.3, the VA interface development required in PWS section 5.4, and the pilot project operation and evaluation support required in PWS section 5.5. The scrum teams for this effort shall be composed of an evolving mix of technical skill sets as required to meet the necessary stage of the software development lifecycle and technical nature of the project. The Contractor shall adjust deliverables and technical Rational updates to match the nature of the software product under development.

These development/configuration efforts may be required within the overall PWS PoP to include the base period as well as each option period. The Contractor shall provide an additional scrum team to address these requirements. This option can be exercised no more than seven times throughout the PoP of this contract.

The scrum team shall follow the VIP, VA system integration and pilot processes described in Sections 5.2 through 5.5 of this PWS.

In addition to installation at additional pilot sites, the current product backlog is provided as an example of the types of functionality that may be included in this optional task:

1. Additional interface development to add data/ scheduling functionality.
2. Capable of accessing a user manual through the app.
3. Capable of providing a Help section accessible within the app which includes at minimum contact information for obtaining online help.
4. Capable of displaying the app version being used.
5. Capable of providing the user an option to end their authentication session.
6. Capable of providing a time based ending of an authenticated session which cannot exceed 15 minutes of inactivity.
7. Capable of providing authenticated user a message prior to their authentication session ending at 14 minutes of inactivity to allow the opportunity to re-establish their session before it expires.
8. Capable of recording attempts at booking even if unsuccessful and allow Veteran to start a new attempt without re-entry of all data
9. Capable of providing the Veteran a notice when any appointment is successfully booked or cancelled.
10. Capable of exporting appointment information to mobile device or electronic calendars using standard calendar formats (e.g., Outlook, iCal).
11. Capable of providing the Veteran appointment reminders about scheduled appointment by email, SMS, and push notifications.
12. Capable of allowing the Veteran to set preferences around appointment reminders and prompts to include method of delivery, timing, and number of messages.
13. Capable of utilizing existing VA business process or attempts types (no new business process or attempt types will be established for this pilot). The OPSS must interact with appointments scheduled in individual VistA instance scheduling packages.
14. Capable of providing a clear indication in VistA when booking or cancelling an appointment of the system/source of the change in the appointment in the related VistA instance

5.10 LICENSES AND HOSTING FOR INSTALLATION AT ADDITIONAL SITES – OPTIONAL TASK

The Contractor shall provide additional OPSS licenses and hosting for pilot testing at additional sites in the event that VA expands the selection of VISNs. This optional task can be exercised for increments of one additional site up to five times throughout the PoP of this contract. This optional task can be exercised up to five times in each option period for renewal of license and hosting agreements obtained for each new site. Additionally, the Contractor shall provide O&M support as described in PWS section 5.7 and subtasks for all additional licenses and hosting services.

Deliverable:

A. Additional OPSS licenses and hosting

5.11 TRANSITION SUPPORT - OPTIONAL TASK

In accordance with the VIP Guide, transition of knowledge and of product to Sustainment occurs at the end of Product Warranty. The Contractor shall provide a plan for 60 days of outgoing transition support for transitioning work from the current contract to a follow-on contract or Government entity. This transition may be to a Government entity or to another Contractor or to the incumbent Contractor under a new contract order. In accordance with the Government-approved plan, the Contractor shall assist the Government in implementing a complete transition from this contract to a new support provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of all artifacts delivered under this contract, as well as existing policies and procedures, and delivery of baseline metrics and statistics. This Transition Plan shall include, but is not limited to:

a) Coordination with Government representatives.
b) Review, evaluation and transition of current support services.
c) Transition of historic data to new Contractor system.
d) Transition of Rational accounts.
e) Transfer of hardware and software warranties, maintenance agreements and licenses.
f) Transfer of all necessary business and/or technical documentation
g) Orientation phase and program to introduce Government and Contractor personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes.
h) Disposition of Contractor purchased Government owned assets,
i) Transfer of Government Furnished Equipment (GFE) and Government Furnished Information, and GFE inventory management assistance.
j) Turn-in of all Government keys, ID/access cards, and security codes.

Deliverable:

A. Transition Plan

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-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 are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, 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 Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) 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. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.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://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

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 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 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 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) specific to the particular client operating system being used.

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

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates 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 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), Federal Bureau of Investigation (FBI) name check, FBI fingerprint check, and written inquiries to

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
	previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

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 / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☒	☐	☐
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.

6.2.2 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.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within three 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 ProPath template. 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.
d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. 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 Security and Investigations Center (SIC) Fingerprint Request Form
f. 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).
g. 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 eQIP).
h. 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.
i. 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), training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." 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 the Office of Personnel Management (OPM).

j. 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.
k. 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.
l. 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 5. 99.99 percent availability of OPSS.	Satisfactory or higher

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. 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 authorized contract staff 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, ProPath, 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

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific contract The Government also understands that GFE is limited to Contractors requiring direct access to the network to: access development environments; install, configure and run TRM-approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner, etc.); upload/download/ manipulate code, run scripts, apply patches, etc.; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

Based on the Government assessment of remote access solutions and the requirements of this contract, the Government estimates that the following GFE will be required by this contract:

1. Five developer-grade laptops

The Government will not provide IT accessories including but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra PIV readers, peripheral devices, additional RAM, etc. The Contractor is responsible for providing these types of IT accessories in support of the contract as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

6.7 SHIPMENT OF HARDWARE OR EQUIPMENT

Not applicable.

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, 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**.**

A2.1. 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.

A3.1. 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 and http://www.section508.gov/content/learn/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

A3.2. 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.

A3.3. 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.

A3.4. 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. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

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. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products.

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*

B1. 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.

B2. 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.

B3. 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 Service Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. 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**,** based upon the severity of the incident.

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 based upon the requirements identified within the contract.

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.

B5. 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.

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 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.

B6. 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.

B7. 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.

B8. 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.

B9. 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) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior,* Appendix D relating to access to VA information and information systems.

2) 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 1 week 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 D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

Attachment 002 - Price Schedule Excel Spreadsheet

SECTION E - SOLICITATION PROVISIONS

E.12 PROPOSAL SUBMISSION

1. INTRODUCTION

The Offeror's proposal shall be submitted electronically via the Virtual Office of Acquisition (VOA) in the files set forth below by the date and time indicated in the Solicitation. Proposals submitted by any other method will not be considered. The Offeror's proposal shall consist of five volumes. The Volumes are I -Technical, II – Past Performance, III – Price, IV – Veterans Involvement, and V - Solicitation, Offer and Award Documents. The use of hyperlinks or embedded attachments in proposals is prohibited. Accordingly, any information contained within an embedded attachment and/or hyperlink will neither be accessed nor evaluated. File sizes shall not exceed 100MB. The web address for the VOA site is https://www.voa.va.gov/. Offerors will be required to be registered users on the VOA website in order to submit proposals. Once registered, Offerors can click on the Proposal Dashboard link and within that link click on Add Proposal to open up the form to upload files. The Proposal Type drop down field should be changed to VA118-17-R-1848 to reflect the solicitation being proposed against. For registration or technical issues concerning proposal submission, contact voahelp@va.gov.
WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

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

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

All files will be submitted as either a Microsoft Excel (.XLS) file or an Acrobat (PDF) file or compatible as indicated in the table. Page size shall be no greater than 8 1/2" x 11" with printing on one side, only. The top, bottom, left and right margins shall be a minimum of one inch (1") each. Font size shall be no smaller than 12-point. Arial or Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos, and headers and footers may be within the page margins ONLY, and are not bound by the 12-point font requirement. Footnotes to text shall not be used. All proprietary information shall be clearly and properly marked. If the Offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the Offeror's page limitations unless otherwise indicated in

the specific volume instructions below. Pages in violation of these instructions, either by exceeding the margin, font or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view.

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

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

Volume Number	**Factor**	**File Name**	**Page Limitations**
Volume I	Technical	(Prime Offeror)_Tech.pdf	~~20~~25
Volume II	Past Performance	(Prime Offeror)_Past Perf.pdf	None
Volume III	Price	(Prime Offeror)_Price.xls	None
Volume IV	Veterans Involvement	(Prime Offeror)_VetsI.pdf	None
Volume V	Solicitation, Offer & Award Documents, Certifications & Representations	(Prime Offeror)_OffRep.pdf	None
	Small Business Subcontracting Plan (LARGE BUSINESS ONLY)	(Prime Offeror)_SBSP.PDF	None

A Cover Page, Table of Contents, glossary of abbreviations or acronyms, and Section E.12~~0~~(2)(c)(i)(6) will not be included in the page count of the Technical Volume. However, be advised that any and all information contained within any Table of Contents and/or glossary of abbreviations or acronyms submitted with an Offeror's proposal will not be evaluated by the Government.

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

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

1. A description of its existing commercially available, off-the-shelf online patient self-scheduling system's capability and approach to meeting each of the congressionally mandated requirements described in Section 5.3 of the PWS.

2. A detailed discussion of its existing commercially available, off-the-shelf online patient self-scheduling system's capability or approach to meeting the current VA scheduling processes defined in PWS Section 5.3 required to meet the seven congressionally mandated requirements. The discussion shall specifically focus on:
   - (~~8~~1) Capable of accessing a calendar / list of available appointments for the authenticated Veteran to book in real-time from specific VA facilities based upon: (a) Veteran identity; (b) Veteran relationship to facility; (c) Capable of reading a Veteran's past appointment history at the facility; (d) Facility-established settings for Veteran direct booking/cancellation of appointments;
   - (~~13~~6) Capable of real-time display of appointment availability, with ability to resolve conflicts and prevent duplicated appointments in an environment where multiple systems may be interacting with VistA, the authoritative scheduling package. Current systems that interact with VistA and can book appointments are the Veteran Scheduling Enhancement Application, Schedule Manager Application, Veteran Appointment Request Application, and VistA Scheduling;
   - (~~14~~7) Capable of capturing the Veteran's preferred date when booking or cancelling an appointment at the beginning of the process; and
   - (~~16~~9) Capable of limiting the scheduling of Primary Care and Mental Health appointments to providers for whom the patient has an existing relationship. Specifically, Primary Care appointments will be scheduled with the Veterans Patient Aligned Care Team (PACT) team using data from the Primary Care Management Module (PCMM) to validate the Primary Care Team relationship. For Mental Health and Specialty Care the Veteran can only schedule with providers with whom they have had appointments in the prior 13 months.

3. A detailed description of all tasks required to integrate its existing commercially available, off-the-shelf online patient self-scheduling system with VA systems in accordance with (IAW) PWS Sections 5.4 and a discussion of potential risks and mitigations. Include a description of data sources and VA interfaces required for successful system integration.

4. A detailed description of the proposed hosting environment including the approach to: Federal Information Security Management Act (FISMA) High and Trusted Internet Connection (TIC) 2.0 compliance IAW PWS paragraph 5.4; and Obtaining an Authority to Operate IAW PWS paragraph 5.5.1.

5. A detailed approach to planning and operating the pilot as described in PWS Section 5.5.2 and 5.5.4

6. Provide a Master Schedule, Work Breakdown Structure, and identify labor categories for the Prime and any proposed team members and/or vendors for PWS Sections 5.3 through 5.7 and their associated subparagraphs.

(ii) VOLUME II – PAST PERFORMANCE FACTOR. Offerors shall submit up to 10 ~~a list of all~~ contracts (including Federal, State, and local government and private) (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation. Areas of relevance include installing, integrating, testing, deploying, and maintaining commercially available, online patient self-scheduling systems relative to the scale of the Faster Care for Veterans Pilot Program or VistA integration. Data

concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order. This volume shall be organized into the following sections:

(1) Section 1 – Contract Descriptions. This section shall include the following information:

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

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

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

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

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

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

(g) Awarded price/cost.

(h) Final or projected final price/cost.

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

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

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

(3) Section 3 – Subcontracts. Offerors shall provide an outline of how the effort required by the solicitation will be assigned for performance within the Offeror's corporate entity and among the proposed subcontractors. The information provided for the prime Offeror and each proposed

major subcontractor must include the entire company name, company address, CAGE Code, DUNS Number and type of work to be performed by citing the applicable Government PWS paragraph number. The Offeror shall identify the percentage of the total proposed price per major subcontractor.

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

(iii) VOLUME III– PRICE/COST FACTOR. The Offeror shall complete the Schedule of Supplies/Services found in the Excel Price Evaluation Spreadsheet. The Total Evaluated Price shall be based on the information provided in the Excel Price Evaluation Spreadsheet. Breakdown of price data is not required in as much as the Contracting Officer anticipates adequate price competition.

a. FFP Line Items, Firm Quantities - The Offeror shall complete the Excel Price Evaluation Spreadsheet by inputting unit prices for every FFP line item in each of the purchase/contract periods, including options. Proposed unit prices shall be no more than two decimal places.

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

c. All Offerors should propose using an estimated award date of April 14, 2017.

(iv) VOLUME IV – VETERANS INVOLVEMENT FACTOR.

(1) For SDVOSBS/VOSBs: In order to receive credit under this Factor, an Offeror shall submit a statement of compliance that it qualifies as a SDVOSB or VOSB in accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors. Offerors are cautioned that they must be registered and verified in Vendor Information Pages (VIP) database (http://www.VetBiz.gov).

(2) For Non-SDVOSBs/VOSBs: To receive some consideration under this Factor, an Offeror must state in its proposal the names of SDVOSB(s) and/or VOSB(s) with whom it intends to subcontract, and provide a brief description and the approximate dollar values of the proposed subcontracts. Additionally, proposed SDVOSB/VOSB subcontractors must be registered and verified in VIP database (http://www.VetBiz.gov) in order to receive some consideration under the Veteran's Involvement Factor.

(3) With regard to the requirements for registration and verification in the VetBiz database, reference VAAR 804.1102.

(4) At the Offeror's sole discretion, and for some consideration under this evaluation factor, provide information in accordance with VAAR Subpart 852.219-72, Evaluation Factor for Participation in the VA Mentor-Protégé Program.

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

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

a. Solicitation Section A – Standard Form (SF1449) and Acknowledgement of Amendments, if any.

b. Any proposed terms and conditions and/or assumptions upon which the proposal is predicated.

c. Offerors shall provide list of all proposed subcontractors including company name, CAGE code and DUNS number.

d. Large Business shall submit a Small Business Subcontracting Plan (SBSP) IAW FAR 52.219-9 and VAAR 852.219-9. The Offeror shall include in its SBSP the extent to which the Offeror meets or exceeds the Government's Subcontracting goals for this procurement, which are as follows: Service-Disabled Veteran-Owned Small Business (SDVOSB): 3.0% of the total contract value; Veteran-Owned Small Business (VOSB): 5.0% of the total contract value; Small Disadvantaged Business (SDB): 5.0% of the total contract value; Women-Owned Small Business: 5.0% of the total contract value; Historically Underutilized Business Zone (HUB Zone) Small Business: 3.0% of the total contract value. Any inability to meet the Government's subcontracting goal(s) or if the Offeror is not proposing to subcontract it shall include detailed rationale to support the determination. If the large business does not have an approved Master Plan or approved Commercial Plan, then an Individual Subcontracting Plan must be submitted that includes an assurance that small businesses will be given the maximum practicable opportunity to participate in contract performance. This plan shall be submitted separately from the Small Business Participation information required above, which applies to both Large and Small businesses. The Subcontracting Plan is not a requirement for evaluation in source selection, but rather, a requirement for award to a Large Business and the Plan, as negotiated, will be incorporated into any resultant contract.

e. Offerors shall provide all proposed commercial license agreements.

Offerors are hereby advised that any Offeror-imposed terms and conditions and/or assumptions which deviate from the Government's material terms and conditions established by the Solicitation, may render the Offeror's proposal Unacceptable, and thus ineligible for award.

E.13 BASIS OF AWARD

Any award will be made based on the best overall (i.e., best value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the four following evaluation Factors: Technical, Past Performance, Price, and Veterans Involvement.

The Technical Factor is significantly more important than the Past Performance Factor, which is significantly more important than the Price Factor, which is slightly more important than the Veterans Involvement Factor. To receive consideration for award, a rating of no less than "Acceptable" must be achieved for the Technical Factor. The non-Price Factors combined are significantly more important than the Price Factor. Offerors are cautioned that the award may not necessarily be made to the lowest Price offered or the most highly rated technical proposal. The Government intends to award a single contract as a result of the evaluations.

E.14 FACTORS TO BE EVALUATED

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

E.15 EVALUATION APPROACH

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

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

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

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

2. PAST PERFORMANCE EVALUATION APPROACH.

The Past Performance evaluation will assess the relative risks associated with an Offeror's likelihood of success in fulfilling the solicitation's requirements as indicated by that Offeror's record of past performance. In this context, “Offeror” refers to the proposed prime contractor and all proposed major subcontractor(s). A major subcontractor is defined as one who will be providing VA system integration (e.g. VistA), pilot testing, operations and maintenance support, or software licenses or whose subcontract is for more than 25 percent of the total proposed price. In either case, the prime contractor and proposed major subcontractor(s) will be assessed individually and the results will then be assessed in their totality to derive the Offeror’s Past Performance rating.

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

The Government will review aspects of cost, schedule and performance. Areas to be evaluated may include but are not limited to quality of product or service, effectiveness of program management (to include use and control of subcontractors), performance against contract metrics, ability to identify and mitigate risks, ability to manage complex projects at multiple geographically dispersed sites, timeliness of performance or adherence to delivery schedules, and commitment to customer satisfaction.

In the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available or is of such limited scope as to not be reliable, the Offeror may not be evaluated favorably or unfavorably on past performance.

3. PRICE EVALUATION APPROACH.

The total overall evaluated price will be the sum of all FFP line items, including all options. The total evaluated price for each FFP line item will be calculated by multiplying the quantity/unit (e.g. 1 LO) by the proposed unit price. The Government will verify the Offeror’s calculation of the total overall evaluated price using the Excel Pricing spreadsheet provided as Attachment 001 to the solicitation. The Government will adjust the Offeror’s proposed total overall evaluated price if mathematical errors are identified.

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

4. VETERANS INVOLVEMENT EVALUATION APPROACH.

In accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business (VOSB) Evaluation Factors, the Government will assign evaluation credit for an Offeror (prime contractor) which is a Service-Disabled Veteran-Owned Small Business (SDVOSB) or a VOSB. Non-SDVOSB/VOSB Offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation Factor. In accordance with VAAR 852.219-72, Evaluation Factor for Participation in the VA Mentor-Protégé Program, non-SDVOSB/VOSBs with approved Mentor-Protégé Agreements.