

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NO.		PAGE 1 OF 167	
2. CONTRACT NO. /		3. AWARD/EFFECTIVE DATE		4. ORDER NO.		5. SOLICITATION NUMBER 36C10B19R0043	
6. SOLICITATION ISSUE DATE 9/3/19		7. FOR SOLICITATION INFORMATION CALL: a. NAME Jamie McPherson		b. TELEPHONE NO. (No Collect Calls) 732-795-1090		8. OFFER DUE DATE/LOCAL TIME 9/10/19 @ 12PM EST	
9. ISSUED BY Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724				10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS: 541512 <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> EDWOSB <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8(A) SIZE STANDARD: \$27.5 Million			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING N/A	
14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input checked="" type="checkbox"/> RFP				15. DELIVER TO See Delivery Schedule Eatontown NJ 07724			
16. ADMINISTERED BY Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724				17a. CONTRACTOR/OFFEROR CODE _____ FACILITY CODE _____			
18a. PAYMENT WILL BE MADE BY Department of Veterans Affairs Technology Acquisition Center Financial Services Center PO Box 149971 Austin TX 78714-8971 PHONE: _____ FAX: _____				17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>			
18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM				19. ITEM NO.			
20. SCHEDULE OF SUPPLIES/SERVICES				21. QUANTITY			
22. UNIT				23. UNIT PRICE			
24. AMOUNT				25. ACCOUNTING AND APPROPRIATION DATA			
26. TOTAL AWARD AMOUNT (For Govt. Use Only)				27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input checked="" type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.			
27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED				28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED			
29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____ YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN IS ACCEPTED AS TO ITEMS:				30a. SIGNATURE OF OFFEROR/CONTRACTOR			
31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)				30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)			
31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT) Juan Quinones Contracting Officer				30c. DATE SIGNED			
31c. DATE SIGNED				32. AUTHORIZED FOR LOCAL REPRODUCTION PREVIOUS EDITION IS NOT USABLE			

Table of Contents

SECTION A	1
A.1 SF 1449 SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS.....	1
SECTION B - CONTINUATION OF SF 1449 BLOCKS.....	6
B.1 GOVERNING LAW	6
B.2 SOFTWARE LICENSE, MAINTENANCE AND TECHNICAL SUPPORT	7
B.3 CONTRACT ADMINISTRATION DATA	9
B.4 PRICE SCHEDULE	10
B.5 PERFORMANCE WORK STATEMENT	61
1.0 BACKGROUND.....	62
2.0 APPLICABLE DOCUMENTS	63
3.0 SCOPE OF WORK	66
4.0 PERFORMANCE DETAILS.....	67
4.1 PERFORMANCE PERIOD	67
4.2 PLACE OF PERFORMANCE	67
4.3 TRAVEL	67
5.0 SPECIFIC TASKS AND DELIVERABLES	68
5.1 PROGRAM MANAGEMENT	68
5.1.1 CONTRACTOR PROGRAM MANAGEMENT PLAN	68
5.1.2 JOINT PROGRAM MANAGEMENT OFFICE	68
5.1.3 GENERAL REPORTING REQUIREMENTS	69
5.1.3.1 CBCESA MONTHLY STATUS REPORTING	69
5.1.3.2 CBCESA SERVICE LEVEL AGREEMENT MONITORING PLAN AND REPORT	69
5.1.4 PROGRAM MEETINGS.....	70
5.1.4.1 TECHNICAL KICKOFF MEETING	70
5.1.4.2 WEEKLY JOINT PROGRAM MANAGEMENT OFFICE MEETING.....	70
5.1.4.3 QUARTERLY STEERING COMMITTEE MEETING.....	70
5.1.4.4 BI-ANNUAL EXECUTIVE PROGRAM MANAGEMENT REVIEWS (PMR) ..	70
5.1.4.5 AD HOC/TIGER TEAM MEETINGS	71
5.2 CISCO SMART NET TOTAL CARE SERVICES	71
5.2.1 TECHNICAL ASSISTANCE CENTER	71
5.2.2 CLASSIFIED NETWORK SERVICES-HIGH TOUCH TECHNICAL SERVICES (CNS-HTTS).....	73
5.2.3 ADVANCED HARDWARE REPLACEMENT	73
5.2.3.1 MISSION CRITICAL SUPPORT UPGRADE.....	73
5.2.4 SOFTWARE DEVELOPERS	75
5.2.5 PRODUCT BUSINESS UNITS	75

5.2.6	PRODUCTIVITY TOOLS AND SOFTWARE.....	75
5.2.7	TROUBLESHOOTING TOOLS AND SUPPORT	76
5.3	CISCO SOFTWARE SUPPORT SERVICES (SWSS) FOR CISCO UNIFIED BORDER ELEMENT (CUBE)S AND CISCO® UNIFIED SESSION INITIATION PROTOCOL (SIP)..	76
5.3.1	CISCO CLOUD SERVICES ROUTER (CSR) 1000v SUPPORT.....	76
5.3.2	SUPPORT EXCLUSIONS	77
5.4	CISCO COLLABORATION FLEX ENTERPRISE SERVICE.....	77
5.4.1	ENTERPRISE CALLING SERVICES	77
5.4.2	ENTERPRISE CONTACT CENTER SERVICES.....	78
5.4.3	CISCO COLLABORATION FLEX ENTERPRISE SUPPORT AND BASE REQUIREMENTS	78
5.5	CISCO BUSINESS CRITICAL SERVICES	80
5.5.1	CISCO OPTIMIZATION SERVICES	80
5.5.2	OPTIMIZATION ENGINEERING SUPPORT	81
5.5.3	SOFTWARE STRATEGY	81
5.5.4	HARDWARE STRATEGY	81
5.5.5	DESIGN STRATEGY.....	81
5.5.6	CHANGE MANAGEMENT STRATEGY	82
5.5.7	SECURITY VULNERABILITY REPORTING	82
5.5.8	HOSTED LAB TEST CYCLES.....	83
5.5.9	ROUTING & SWITCHING OPTIMIZATION SERVICE	84
5.5.9.1	ARCHITECTURE DESIGN REVIEW	84
5.5.9.2	STABILITY AUDIT	84
5.5.10	BUSINESS ROUTING AND SWITCHING STRATEGY CONSULTING	85
5.5.11	UNIFIED COMMUNICATIONS OPTIMIZATION SERVICE.....	85
5.5.11.1	ARCHITECTURE DESIGN REVIEW	85
5.5.11.2	SYSTEM ANALYSIS	86
5.5.11.3	STABILITY AUDIT.....	86
5.5.12	BUSINESS UNIFIED COMMUNICATION CONSULTING.....	87
5.5.13	DATA CENTER/UNIFIED COMPUTING OPTIMIZATION SERVICE.....	87
5.5.13.1	ARCHITECTURE DESIGN REVIEW (ADR)	87
5.5.13.2	STABILITY AUDIT.....	88
5.5.14	BUSINESS CISCO DATA CENTER/COMPUTING CONSULTING	89
5.5.15	WIRELESS LANS OPTIMIZATION SERVICE.....	89
5.5.15.1	ARCHITECTURE DESIGN REVIEW	89
5.5.15.2	STABILITY AUDIT.....	90
5.5.16	BUSINESS CISCO WIRELESS LAN NETWORK CONSULTING.....	90
5.5.17	TELEPRESENCE (BUSINESS VIDEO) OPTIMIZATION SERVICE	91
5.5.17.1	ARCHITECTURE/STABILITY REVIEW-EVTN.....	91
5.5.18	BUSINESS VIDEO STRATEGY CONSULTING.....	91
5.5.19	CISCO FOCUSED TECHNICAL SUPPORT SERVICES	92
5.5.19.1	HIGH TOUCH OPERATIONS MANAGER	92
5.5.19.2	CASE MANAGEMENT	92

5.5.19.3	ASSET AND CISCO PORTAL MANAGEMENT SUPPORT.....	93
5.5.19.4	INVENTORY COLLECTION TOOLS	93
5.5.19.5	CISCO DIGITAL NETWORK ARCHITECTURE (DNA) CENTER DASHBOARD AND APPLIANCE LIMITED SUPPORT	94
5.5.20	KNOWLEDGE TRANSFER, MENTORING, AND TRAINING SUPPORT	94
5.5.20.1	GENERAL KNOWLEDGE TRANSFERS.....	94
5.5.20.2	CISCO LEARNING CREDITS	95
5.5.20.3	TECHNICAL KNOWLEDGE LIBRARY (TKL)	96
5.5.20.4	CISCO PLATINUM LEARNING LIBRARY (CPLL) ACCESS	96
5.5.20.5	CISCO MODELING LABS (CML) CORPORATE EDITION PLATFORM	97
5.5.21	CBCESA INVENTORY MANAGEMENT.....	97
5.5.21.1	MASTER INVENTORY REPORTING	97
5.5.21.2	INSTALL BASE REPORT	97
5.5.21.3	CISCO COLLABORATION FLEX SERVICE REPORT.....	98
5.5.21.4	CBCESA INVENTORY RECONCILIATION/TRUE-UP AND TRUE- FORWARD	98
5.5.21.5	INSTALL BASE RECONCILIATION/TRUE-UP PROCESS	98
5.5.21.6	CISCO COLLABORATION FLEX SERVICE INVENTORY TRUE-FORWARD PROCESS.....	100
5.5.22	CBCESA USER ACCESS AND REPORTING	100
5.6	SYSTEM AND ORGANIZATIONAL CONTROLS (SOC) FOR SERVICE ORGANIZATIONS REPORTING REQUIREMENTS	101
5.6.1	SERVICE ORGANIZATION CONTROL (SOC) REPORTING	101
5.6.2	SERVICE ORGANIZATION CONTROL REPORTING - SPECIFICATIONS AND DELIVERABLES	101
5.7	RIGHTS IN COMMERCIAL LICENSES AND TECHNICAL DATA AND REPORTS	103
6.0	GENERAL REQUIREMENTS	103
6.1	ENTERPRISE AND IT FRAMEWORK.....	103
6.1.1	VA TECHNICAL REFERENCE MODEL	103
6.1.2	FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 103	
6.1.3	INTERNET PROTOCOL VERSION 6 (IPV6)	104
6.1.4	TRUSTED INTERNET CONNECTION (TIC).....	105
6.1.5	STANDARD COMPUTER CONFIGURATION	105
6.1.6	VETERAN FOCUSED INTEGRATION PROCESS (VIP).....	105
6.1.7	PROCESS ASSETT LIBRARY (PAL).....	106
6.1.8	AUTHORITATIVE DATA SOURCES	106
6.2	SECURITY AND PRIVACY REQUIREMENTS	107
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S).....	107
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS	107
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES.....	109
6.4	PERFORMANCE METRICS.....	109

6.4.1 DELIVERABLE METRICS/SERVICE LEVEL AGREEMENTS (SLA)	110
6.5 FACILITY/RESOURCE PROVISIONS	112
6.6 GOVERNMENT FURNISHED PROPERTY	113
ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED.....	115
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE	121
SECTION C - CONTRACT CLAUSES.....	131
C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998).....	131
C.2 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (AUG 2019)	132
C.3 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)	139
SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS	140
SECTION E - SOLICITATION PROVISIONS.....	141
E.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)	141
E.2 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL ITEMS (OCT 2018).....	141
E.3 52.216-1 TYPE OF CONTRACT (APR 1984)	159
E.4 52.233-2 SERVICE OF PROTEST (SEP 2006)	159
E.5 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (OCT 2018)	160
E.6 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (OCT 2018).....	160
E.7 BASIS FOR AWARD	161
E. 8 FACTORS TO BE EVALUATED.....	161
E.9 EVALUATION APPROACH	161
E.10 PROPOSAL SUBMISSION	163

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Order. Commercial license agreements may be made a part of this Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (*e.g.*, restricted computer software) are included and made a part of this Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 *et seq.*), the Anti-Deficiency Act (31 U.S.C. § 1341 *et seq.*), the Competition in Contracting Act (41 U.S.C. § 3301 *et seq.*), the Prompt Payment Act (31 U.S.C. § 3901 *et seq.*), Contracts for Data Processing or Maintenance (38 USC § 5725), and FAR clauses 52.212-4, 52.227-14, 52.227-19 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this Clause and any provision in the Order or the commercial license agreement or elsewhere, the terms of this Clause shall prevail. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 28 U.S.C. § 516. At the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Order must be made by contract/order modification (Standard Form 30) and shall only be effected by a warranted Contracting Officer. Nothing in this Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.2 SOFTWARE LICENSE, MAINTENANCE AND TECHNICAL SUPPORT

(1) Definitions.

(a) Licensee. The term “licensee” shall mean the U.S. Department of Veterans Affairs (“VA”) and is synonymous with “Government.”

(b) Licensor. The term “licensor” shall mean the contractor having the necessary license or ownership rights to deliver license, software maintenance and support of the computer software being acquired. The term “contractor” is the party identified in Block 17a on the SF1449. If the contractor is a reseller and not the Licensor, the contractor remains responsible for performance under this order.

(c) Software. The term “software” shall mean the licensed computer software product(s) cited in the Schedule of Supplies/Services.

(d) Maintenance. The term “maintenance” is the process of enhancing and optimizing software, as well as remedying defects. It shall include all new fixes, patches, releases, updates, versions and upgrades, as further defined below.

(e) Technical Support. The term “technical support” refers to the range of services providing assistance for the software via the telephone, email, a website or otherwise.

(f) Release or Update. The term “release” or “update” are terms that refer to a revision of software that contains defect corrections, minor enhancements or improvements of the software’s functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.

(g) Version or Upgrade. The term “version” or “upgrade” are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

(2) Software License

(a) Unless otherwise stated in the Schedule of Supplies/Services, the Performance Work Statement or Product Description, the software license provided to the Government is a perpetual, nonexclusive license to use the software

(b) The Government may use the software in a networked environment. Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).

All limitation of software usage are expressly stated in the Schedule of Supplies/Services and the Performance Work Statement/Product Description.

(3) Software Maintenance and Technical Support

(a) If the Government desires to continue software maintenance and support beyond the period of performance identified in this contract or order, the Government will issue a separate contract or order for maintenance and support. Conversely, if a contract or order for continuing software maintenance and technical support is not received the contractor is neither authorized nor permitted to renew any of the previously furnished services.

(b) The contractor shall provide software support services, which includes periodic updates, enhancements and corrections to the software, and reasonable technical support, all of which are customarily provided by the contractor to its commercial customers so as to cause the software to perform according to its specifications, documentation or demonstrated claims.

(c) Any telephone support provided by contractor shall be at no additional cost.

(d) The contractor shall provide all maintenance services in a timely manner in accordance with the contractor’s customary practice or as defined in the Performance Work Statement/Product Description. However, prolonged delay (exceeding 2 business days) in resolving software problems will be noted in the Government’s various past performance records on the contractor (e.g., www.ppirs.gov).

(e) If the Government allows the maintenance and support to lapse and subsequently wishes to reinstate it, any reinstatement fee charged shall not exceed the amounts that would have been charged if the Government had not allowed the subscription to lapse.

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

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

B.3 CONTRACT ADMINISTRATION DATA

(continuation from Standard Form 1449, block 18A.)

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

- a. CONTRACTOR: To Be Determined.
- b. GOVERNMENT: Contracting Officer 36C10B
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

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

- [X] 52.232-33, Payment by Electronic Funds Transfer—System for Award Management, or

3. INVOICES: Invoices shall be submitted in arrears:

- a. Quarterly ☐
- b. Semi-Annually ☐
- c. Other ☒ Upon acceptance of Deliverables, IAW Section B.4, Price Schedule

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

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

AMENDMENT NO	DATE

B.4 PRICE SCHEDULE

All deliverables must be submitted electronically 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 Numbers (CLIN) 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.

The Contractor shall meet all Deliverable Metrics/Service Level Agreements (SLA) as described in the Performance Work Statement (PWS). However, if the Contractor's performance falls below a required service level, the Contractor shall only be paid for the lower service level provided. See Section B.5 Performance Work Statement, Section 6.4.1 for Deliverable Metrics/SLA Performance.

NOTE: Vendors are instructed to see solicitation Section E for proposal submission instructions inclusive of the price proposal. Section B.4 Price schedule is for informational purposes only for solicitation. Vendors are cautioned that alterations to the line items as specified below may render quotes unacceptable. All questions shall be directed to the Contract Jamie McPherson, Jamie.McPherson@va.gov and Contracting Officer, Juan Quinones, Juan.Quinones@va.gov prior to the closing date and time specified in the Request for Proposal (RFP).

F.O.B.: Destination

Inspection/Acceptance: Destination

Electronic Submission to: VA PM, COR, and CO

BASE PERIOD

Period of Performance (PoP) shall be 12 months from the date of award.

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
0001	<p>Program Management in accordance with (IAW) Performance Work Statement (PWS) 5.1.</p> <p>Period of performance (PoP) is 12 months from date of award.</p> <p>The Price of this Contract Line Item Number (CLIN) and its Sub Contract Line Item Numbers (SLIN) shall be allocated to CLINs 0002 and 0004</p>	12	MO	NSP	NSP

0001AA	Contract Project Management Plan IAW paragraph 5.1.1 of the Performance Work Statement. Due 10 business days after receipt of contract. The Contractor shall update and maintain and deliver the CPMP throughout the period of performance.	1	LO	NSP	NSP
0001AB	Contractor Staff Support Roster IAW paragraph 5.1.2 of the PWS. Due within five business days of a change or one business day prior to weekly Joint Program Management Office (JPMO) Meeting.	1	LO	NSP	NSP
0001AC	Cisco Business Critical Enterprise Service Agreement (CBCESA) Monthly Status Report IAW paragraph 5.1.3.1 of the PWS. Due monthly throughout the PoP. The CBCESA Monthly Status Report shall be delivered the last day of the preceding month.	12	MO	NSP	NSP
0001AD	CBCESA Service Level Agreement (SLA) Monitoring Plan IAW paragraph 5.1.3.2 of the PWS. Due within 15 business days of award and updated periodically thereafter	12	MO	NSP	NSP
0001AE	CBCESA SLA Monitoring Report IAW paragraph 5.1.3.2 of the PWS. Due monthly after first 30 business days of award and updated periodically thereafter	12	MO	NSP	NSP
0001AF	Technical Kickoff Meeting Minutes IAW paragraph 5.1.4.1 of the PWS. Due within five business days after the Kickoff Meeting.	1	EA	NSP	NSP
0001AG	Weekly Joint Program Management Office (JPMO) Meeting Minutes IAW paragraph 5.1.4.2 of the PWS. Due one day prior to the next meeting or within three business days, whichever comes first.	52	EA	NSP	NSP

0001AH	Steering Committee Slides/Minutes IAW paragraph 5.1.4.3 of the PWS. Due No Later Than (NLT) four hours prior to the Steering Committee Meeting throughout the PoP.	4	EA	NSP	NSP
0001AJ	Bi-Annual PMR Minutes IAW paragraph 5.1.4.4 of the PWS. Due within five business days after the meeting.	2	EA	NSP	NSP
0001AK	Ad-Hoc/Tiger Team Meeting Minutes IAW paragraph 5.1.4.5 of the PWS. Due one day prior to the next meeting or within five business days, whichever comes first	1	LO	NSP	NSP
0002	Cisco Base Services (SmartNet Total Care, Software Support Service, Business Critical Services) IAW PWS paragraphs 5.2, 5.3, 5.5, 5.6 and their subtasks. Install Base Band (\$ Million): \$800M – \$900M PoP: 12 months from date of award.	12	MO	\$	\$
0002AA	Mission Critical Device Listing IAW PWS paragraphs 5.2.3.1. Due within 48 hours of request from COR and on a 6-month basis.	1	LO	NSP	NSP
0003	Cisco Software Support Services (SWSS) for Cisco Collaboration Edge and Unified Session Initiation Protocol (SIP)Proxy IAW PWS paragraph 5.3 and its subtasks. PoP: 12 months from date of award. The Price for this CLIN shall be allocated to CLIN 0002	12	MO	NSP	NSP
0004	Cisco Collaboration Flex Enterprise Service IAW PWS paragraphs 5.4 and its subtasks. Collaboration Flex Band (Knowledge Workers (KW)):	12	MO	\$	\$

	260,000 - 311,999 KWs PoP: 12 months from date of award.				
0004AA	Collaboration Flex Enterprise Service Workspace IAW PWS paragraph 5.4.3. Due within 30 business days of award.	1	EA	NSP	NSP
0005	Cisco Business Critical Services IAW PWS Paragraphs 5.5 and its subtasks. PoP: 12 months from date of award. The Price for this CLIN and it its SLINs shall be allocated to CLIN 0002	12	MO	NSP	NSP
0005AA	Contractor/Network Consulting Engineering (NCE) Support Team Roster(s) IAW PWS paragraph 5.5.1 of the PWS. Due quarterly after the date of award.	1	LO	NSP	NSP
0005AB	Solution Delivery (SD) and Infrastructure Operations (IO) Documentation Reviews IAW PWS paragraph 5.5.5. Due within 10 business days of meeting.	1	LO	NSP	NSP
0005AC	Change Management Strategy Report IAW PWS paragraph 5.5.6. Due 180 days after award	1	LO	NSP	NSP
0005AD	Monthly Security Vulnerability/Common Services Platform Collector (CSPC) Report IAW PWS paragraph 5.5.7. Due Monthly throughout the PoP.	12	EA	NSP	NSP
0005AE	Hosted Lab Test Cycles Solution Requirement Document (SRD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request	1	LO	NSP	NSP
0005AF	Hosted Lab Low Level Design Document (LLD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request	1	LO	NSP	NSP

0005AG	Hosted Lab Test Plan IAW PWS paragraph 5.5.8. Due within 10 business days of VA request	1	LO	NSP	NSP
0005AH	Hosted Lab Test Reports IAW PWS paragraph 5.5.8. Due within 15 business days after testing is completed	1	LO	NSP	NSP
0005AJ	Hosted Lab Status Reporting IAW PWS paragraph 5.5.8. Due monthly as part of CLIN 0001AC	1	LO	NSP	NSP
0005AK	Routing and Switching Architecture Design Review Report IAW PWS paragraph 5.5.9.1. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
0005AL	Routing and Switching Stability Audit Report IAW PWS paragraph 5.5.9.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
0005AM	Routing and Switching Network Strategy Report IAW PWS paragraph 5.5.10. Due within 60 days of the topic being provided by VA.	4	EA	NSP	NSP
0005AN	Routing and Switching Consulting Sessions IAW PWS paragraph 5.5.10. The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	3	EA	NSP	NSP
0005AP	Unified Communications (UC) Architecture Design Review Report IAW PWS paragraph 5.5.11.1. Due quarterly throughout the PoP.		LO	NSP	NSP
0005AQ	UC System Analysis Report IAW PWS paragraph 5.5.11.2.	1	LO	NSP	NSP

	Due within 60 days of the topic being provided by VA				
0005AR	UC Stability Audit Report IAW PWS paragraph 5.5.11.3. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
0005AS	UC Consulting Sessions IAW PWS paragraph 5.5.12. The Contractor shall deliver up to two strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	2	EA	NSP	NSP
0005AT	UC Infrastructure Strategy Roadmap Report IAW PWS paragraph 5.5.12 of the PWS. The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	2	EA	NSP	NSP
0005AU	Data Center/Unified Computing Architectural Assessment Plan (AAP) IAW PWS paragraph 5.5.13.1. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005AV	Data Center/Unified Computing Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	5	EA	NSP	NSP
0005AW	Data Center/Unified Computing Consolidated Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP

0005AX	Data Center/Unified Computing Stability Audit Report IAW paragraph 5.5.13.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005AY	Data Center/Computing Infrastructure Strategy Roadmap Report IAW paragraph 5.5.14 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005AZ	Wireless LAN Architecture Design Review Report IAW paragraph 5.5.15.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005BA	Wireless LAN Stability Audit Report IAW paragraph 5.5.15.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005BB	Wireless LAN Network Infrastructure Strategy Roadmap Report IAW paragraph 5.5.16 of the PWS. Due within 60 days of the topic/location being provided by the VA.	4	EA	NSP	NSP
0005BC	Enterprise Video Teleconferencing Network (EVTN) Architecture/Stability Review Report IAW paragraph 5.5.17.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005BD	EVTN Business Video Strategy Roadmap Report IAW paragraph 5.5.18 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
0005BE	Common Services Platform Collector / Telepresence Management System Derived Improvement Report IAW paragraph 5.5.19.4 of the PWS	1	EA	NSP	NSP

	Due within three (3) business days of request by VA, but no less than quarterly.				
0005BF	Cisco DNA Appliance Report IAW paragraph 5.5.19.5 of the PWS Due within 30 business days of award.	1	LO	NSP	NSP
0005BG	Monthly Knowledge Transfer Sessions IAW paragraph 5.5.20.1 of the PWS Due to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	12	MO	NSP	NSP
0005BH	White Papers IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BJ	Design Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BK	Case Studies IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BL	Support and Configuration Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BM	Troubleshooting Guides IAW paragraph 5.5.20.1 of the PWS	1	LO	NSP	NSP

	Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.				
0005BN	Deployment Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BP	Training Documents IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
0005BQ	Cisco Learning Credits (CLC) IAW paragraph 5.5.20.2 of the PWS The Government will authorize additional CLCs over and above the 5,125 CLCs provided with the install base price on an as-needed basis not to exceed 13,125 CLCs throughout the performance of the base period. At the conclusion of the base period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the base period. Initial base set of 5,125 CLCs are due within 30 business days of award. Additional 2,000 CLC packs shall be delivered within 10 business days of request.	NTE 13,125	EA	\$	NTE\$
0005BR	Cisco Platinum Learning Library Licenses IAW paragraph 5.5.20.4 of the PWS Due within 30 business days of award.	200	EA	NSP	NSP
0005BS	Annual Cisco Modeling Labs Licenses IAW paragraph 5.5.20.5 of the PWS	2	EA	NSP	NSP

	Due within 30 business days of award or business days prior to end of license term period.				
0005BT	Install Base Inventory Database Report IAW paragraph 5.5.21.2 of the PWS Due Quarterly and final due within 60 days prior to the end of the PoP	1	LO	NSP	NSP
0005BU	Cisco Collaboration Flex Service Report IAW paragraph 5.5.21.3 Due Quarterly and final due within 60 days prior to the end of the PoP.	4	EA	NSP	NSP
0005BU	CBCESA User Access Report IAW paragraph 5.5.22 of the PWS. Due 180 days after award	1	LO	NSP	NSP
0006	CBCESA Prime Report and Subcontractor Reports IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP
0006AA	CBCESA Service Organization Control Bridge Letter IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP
0007	ISO/IEC 27001 Certification IAW Addendum B, Section B4. Due annually	1	EA	NSP	NSP
TOTAL BASE PERIOD PRICE					\$

OPTION PERIOD ONE

This 12-month option may be exercised in accordance with 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.

Period of performance: October 1, 2020 through September 30, 2021

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
1001	<p>Program Management in accordance with (IAW) Performance Work Statement (PWS) 5.1.</p> <p>Period of performance (PoP): 12 months from date of option exercise.</p> <p>The Price of this Contract Line Item Number (CLIN) and its Sub Contract Lin Item Numbers (SLIN) shall be allocated to CLINs 1002 and 1004.</p>	12	MO	NSP	NSP
1001AA	<p>Contract Project Management Plan IAW paragraph 5.1.1 of the PWS.</p> <p>The Contractor shall update and maintain and deliver the CPMP throughout the period of performance.</p>	1	LO	NSP	NSP
1001AB	<p>Contractor Staff Support Roster IAW paragraph 5.1.2 of the PWS.</p> <p>Due within five business days of a change or one business day prior to weekly Joint Program Management Office (JPMO) Meeting.</p>	1	LO	NSP	NSP
1001AC	<p>Cisco Business Critical Enterprise Service Agreement (CBCESA) Monthly Status Report IAW paragraph 5.1.3.1 of the PWS.</p> <p>Due monthly throughout the PoP. The CBCESA Monthly Status Report shall be delivered the last day of the preceding month.</p>	12	MO	NSP	NSP
1001AD	<p>CBCESA Service Level Agreement (SLA) Monitoring Plan IAW paragraph 5.1.3.2 of the PWS.</p> <p>Due within 15 business days of award and updated periodically thereafter.</p>	12	MO	NSP	NSP
1001AE	CBCESA SLA Monitoring Report IAW paragraph 5.1.3.2 of the PWS.	12	MO	NSP	NSP

	Due monthly after first 30 business days of award and updated periodically thereafter.																				
1001AF	Weekly Joint Program Management Office JPMO Meeting Minutes IAW paragraph 5.1.4.2 of the PWS. Due one day prior to the next meeting or within three business days, whichever comes first.	52	EA	NSP	NSP																
1001AG	Steering Committee Slides/Minutes IAW paragraph 5.1.4.3 of the PWS. Due No Later Than (NLT) four hours prior to the Steering Committee Meeting throughout the PoP.	4	EA	NSP	NSP																
1001AH	Bi-Annual PMR Minutes IAW paragraph 5.1.4.4 of the PWS. Due within five business days after the meeting.	2	EA	NSP	NSP																
1001AJ	Ad-Hoc/Tiger Team Meeting Minutes IAW paragraph 5.1.4.5 of the PWS. Due one day prior to the next meeting or within five business days, whichever comes first.	1	LO	NSP	NSP																
1002	Cisco Base Services (SmartNet Total Care, Software Support Service, Business Critical Services) IAW PWS paragraphs 5.2, 5.3, 5.5, 5.6 and their subtasks. The annual Reconciliation/true-up IAW PWS 5.5.21.5 will establish the IB inventory and Lot Price for Option Period 1. Install Base Band (\$ Million): <table><tr><th>Install Base Bands (\$M)</th><th>Lot Price</th></tr><tr><td>500 - 600</td><td>\$</td></tr><tr><td>600 - 700</td><td>\$</td></tr><tr><td>700 - 800</td><td>\$</td></tr><tr><td>800 - 900</td><td>\$</td></tr><tr><td>900 - 1000</td><td>\$</td></tr><tr><td>1000 - 1100</td><td>\$</td></tr><tr><td>1100 - 1200</td><td>\$</td></tr></table>	Install Base Bands (\$M)	Lot Price	500 - 600	\$	600 - 700	\$	700 - 800	\$	800 - 900	\$	900 - 1000	\$	1000 - 1100	\$	1100 - 1200	\$	12	MO	\$	\$
Install Base Bands (\$M)	Lot Price																				
500 - 600	\$																				
600 - 700	\$																				
700 - 800	\$																				
800 - 900	\$																				
900 - 1000	\$																				
1000 - 1100	\$																				
1100 - 1200	\$																				

	<table><tr><td>1200 - 1350</td><td>\$</td></tr><tr><td>1350 - 1500</td><td>\$</td></tr></table>	1200 - 1350	\$	1350 - 1500	\$										
1200 - 1350	\$														
1350 - 1500	\$														
	PoP: 12 months from date of award.														
1002AA	Mission Critical Device Listing IAW PWS paragraphs 5.2.3.1. Due within 48 hours of request from COR and on a 6-month basis.	1	LO	NSP	NSP										
1003	Cisco Software Support Services (SWSS) for Cisco Collaboration Edge and Unified SIP Proxy IAW PWS paragraph 5.3 and its subtasks. PoP: 12 months from exercise of option year. The Price for this CLIN shall be allocated to CLIN 1002.	12	MO	NSP	NSP										
1004	Cisco Collaboration Flex Enterprise Service IAW PWS paragraphs 5.4 and its subtasks. The annual Reconciliation/true-forward IAW PWS 5.5.21.6 will establish the price for Cisco Collaboration Flex Services in Option Period 1. Collaboration Flex Band (Knowledge Workers (KW)): <table><tr><td>Knowledge Workers (KW) Units Bands</td><td>Lot Price</td></tr><tr><td>260,000 - 311,999</td><td>\$</td></tr><tr><td>312,000 - 374,399</td><td>\$</td></tr><tr><td>374,400 - 449,279</td><td>\$</td></tr><tr><td>449,280 - 539,140</td><td>\$</td></tr></table> PoP: 12 months from exercise of option year.	Knowledge Workers (KW) Units Bands	Lot Price	260,000 - 311,999	\$	312,000 - 374,399	\$	374,400 - 449,279	\$	449,280 - 539,140	\$	12	MO	\$	\$
Knowledge Workers (KW) Units Bands	Lot Price														
260,000 - 311,999	\$														
312,000 - 374,399	\$														
374,400 - 449,279	\$														
449,280 - 539,140	\$														
1004AA	Collaboration Flex Enterprise Service Workspace IAW PWS paragraph 5.4.3. Due within 30 business days of exercise of option year.	1	LO	NSP	NSP										
1005	Cisco Business Critical Services IAW PWS Paragraphs 5.5 and its subtasks. PoP: 12 months from date of award.	12	MO	NSP	NSP										

	The Price for this CLIN and it its SLINs shall be allocated to CLIN 1002.				
1005AA	Contractor/Network Consulting Engineering (NCE) Support Team Roster(s) IAW PWS paragraph 5.5.1 of the PWS. Due quarterly after exercise of option year.	1	LO	NSP	NSP
1005AB	Solution Delivery (SD) and Infrastructure Operations (IO) Documentation Reviews IAW PWS paragraph 5.5.5. Due within 10 business days of meeting.	1	LO	NSP	NSP
1005AC	Change Management Strategy Report IAW PWS paragraph 5.5.6. Due 180 days after award	1	LO	NSP	NSP
1005AD	Monthly Security Vulnerability/Common Services Platform Collector (CSPC) Report IAW PWS paragraph 5.5.7. Due monthly throughout the PoP.	12	MO	NSP	NSP
1005AE	Hosted Lab Test Cycles Solution Requirement Document (SRD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
1005AF	Hosted Lab Low Level Design Document (LLD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
1005AG	Hosted Lab Test Plan IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
1005AH	Hosted Lab Test Reports IAW PWS paragraph 5.5.8. Due within 15 business days after testing is completed.	1	LO	NSP	NSP

1005AJ	Hosted Lab Status Reporting IAW PWS paragraph 5.5.8. Due monthly as part of CLIN 1001AC.	1	LO	NSP	NSP
1005AK	Routing and Switching Architecture Design Review Report IAW PWS paragraph 5.5.9.1. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
1005AL	Routing and Switching Stability Audit Report IAW PWS paragraph 5.5.9.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
1005AM	Routing and Switching Network Strategy Report IAW PWS paragraph 5.5.10. Due within 60 days of the topic being provided by VA.	4	EA	NSP	NSP
1005AN	Routing and Switching Consulting Sessions IAW PWS paragraph 5.5.10. The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
1005AP	Unified Communications (UC) Architecture Design Review Report IAW PWS paragraph 5.5.11.1. Due quarterly throughout the PoP.	1	LO	NSP	NSP
1005AQ	UC System Analysis Report IAW PWS paragraph 5.5.11.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
1005AR	UC Stability Audit Report IAW PWS paragraph 5.5.11.3. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP

1005AS	<p>UC Consulting Sessions IAW PWS paragraph 5.5.12.</p> <p>The Contractor shall deliver up to two strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
1005AT	<p>UC Infrastructure Strategy Roadmap Report IAW PWS paragraph 5.5.12 of the PWS.</p> <p>The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
1005AU	<p>Data Center/Unified Computing Architectural Assessment Plan (AAP) IAW PWS paragraph 5.5.13.1.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP
1005AV	<p>Data Center/Unified Computing Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	5	EA	NSP	NSP
1005AW	<p>Data Center/Unified Computing Consolidated Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP
1005AX	<p>Data Center/Unified Computing Stability Audit Report IAW paragraph 5.5.13.2 of the PWS.</p>	1	EA	NSP	NSP

	Due within 60 days of the topic/location being provided by the VA.				
1005AY	Data Center/Computing Infrastructure Strategy Roadmap Report IAW paragraph 5.5.14 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
1005AA	Wireless LAN Architecture Design Review Report IAW paragraph 5.5.15.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
1005BA	Wireless LAN Stability Audit Report IAW paragraph 5.5.15.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
1005BB	Wireless LAN Network Infrastructure Strategy Roadmap Report IAW paragraph 5.5.16 of the PWS. Due within 60 days of the topic/location being provided by the VA.	4	EA	NSP	NSP
1005BC	Enterprise Video Teleconferencing Network (EVTN) Architecture/Stability Review Report IAW paragraph 5.5.17.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
1005BD	EVTN Business Video Strategy Roadmap Report IAW paragraph 5.5.18 of the PWS. Due within 60 days of the topic/location being provided by the VA	1	EA	NSP	NSP
1005BE	Common Services Platform Collector / Telepresence Management System	1	EA	NSP	NSP

	Derived Improvement Report IAW paragraph 5.5.19.4 of the PWS Due within three (3) business days of request by VA, but no less than quarterly.				
1005BF	Cisco DNA Appliance Report IAW paragraph 5.5.19.5 of the PWS Due within 30 business days of award.	1	EA	NSP	NSP
1005BG	Monthly Knowledge Transfer Sessions IAW paragraph 5.5.20.1 of the PWS Due to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
1005BH	White Papers IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
1005BJ	Design Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
1005BK	Case Studies IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
1005BL	Support and Configuration Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP

1005BM	<p>Troubleshooting Guides IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	1	LO	NSP	NSP
1005BN	<p>Deployment Guides IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	10	EA	NSP	NSP
1005BP	<p>Training Documents IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	1	LO	NSP	NSP
1005BQ	<p>Cisco Learning Credits (CLCs) IAW paragraph 5.5.20.2 of the PWS</p> <p>The Government will authorize additional CLCs over and above the 5,125 CLCs provided with the install base price on an as-needed basis not to exceed 13,125 CLCs throughout the performance of the base period. At the conclusion of the base period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the base period.</p> <p>Initial base set of CLCs are due within 30 business days of award. Additional 2,000 CLC packs shall be delivered within 10 business days of request.</p>	NTE 13,125	EA	\$	\$
1005BR	<p>Cisco Platinum Learning Library Licenses IAW paragraph 5.5.20.4 of the PWS</p> <p>Due within 30 business days of exercise of option year.</p>	200	EA	NSP	NSP

1005BS	Annual Cisco Modeling Labs Licenses IAW paragraph 5.5.20.5 of the PWS Due within 30 business days of award or business days prior to end of license term period.	2	EA	NSP	NSP
1005BT	Install Base Inventory Database Report IAW paragraph 5.5.21.2 of the PWS Due Quarterly and final due within 60 days prior to the end of the PoP	1	LO	NSP	NSP
1005BU	Cisco Collaboration Flex Service Report IAW paragraph 5.5.21.3 Due Quarterly and final due within 60 days prior to the end of the PoP.	4	EA	NSP	NSP
1005BV	CBCESA User Access Report IAW paragraph 5.5.22 of the PWS. Due 180 days after award	1	LO	NSP	NSP
1006	CBCESA Prime Report and Subcontractor Reports IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract	1	EA	NSP	NSP
1006AA	CBCESA Service Organization Control Bridge Letter IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP
1007	ISO/IEC 27001 Certification IAW Addendum B, Section B4. Due annually	1	EA	NSP	NSP
TOTAL OPTION PERIOD ONE					\$

OPTION PERIOD TWO

This 12-month option may be exercised in accordance with 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 option period one. .

Period of performance: October 1, 2021 through September 30, 2022

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
2001	<p>Program Management in accordance with (IAW) Performance Work Statement (PWS) 5.1.</p> <p>Period of performance (PoP): 12 months from date of option exercise.</p> <p>The Price of this Contract Line Item Number (CLIN) and its Sub Contract Lin Item Numbers (SLIN) shall be allocated to CLINs 2002 and 2004</p>	12	MO	NSP	NSP
2001AA	<p>Contract Project Management Plan IAW paragraph 5.1.1 of the Performance Work Statement.</p> <p>The Contractor shall update and maintain and deliver the CPMP throughout the period of performance.</p>	1	LO	NSP	NSP
2001AB	<p>Contractor Staff Support Roster IAW paragraph 5.1.2 of the PWS.</p> <p>Due within five business days of a change or one business day prior to weekly Joint Program Management Office (JPMO) Meeting.</p>	1	LO	NSP	NSP
2001AC	<p>Cisco Business Critical Enterprise Service Agreement (CBCESA) Monthly Status Report IAW paragraph 5.1.3.1 of the PWS.</p> <p>Due monthly throughout the PoP. The CBCESA Monthly Status Report shall be delivered the last day of the preceding month.</p>	12	MO	NSP	NSP
2001AD	<p>CBCESA Service Level Agreement (SLA) Monitoring Plan IAW paragraph 5.1.3.2 of the PWS.</p> <p>Due within 15 business days of award and updated periodically thereafter</p>	12	MO	NSP	NSP
2001AE	<p>CBCESA SLA Monitoring Report IAW paragraph 5.1.3.2 of the PWS.</p>	12	MO	NSP	NSP

	Due monthly after first 30 business days of award and updated periodically thereafter																
2001AF	Technical Kickoff Meeting Minutes IAW paragraph 5.1.4.1 of the PWS. Due within five business days after the Kickoff Meeting.	1	EA	NSP	NSP												
2001AG	Weekly Joint Program Management Office JPMO Meeting Minutes IAW paragraph 5.1.4.2 of the PWS. Due one day prior to the next meeting or within three business days, whichever comes first.	12	MO	NSP	NSP												
2001AH	Steering Committee Slides/Minutes IAW paragraph 5.1.4.3 of the PWS. Due No Later Than (NLT) four hours prior to the Steering Committee Meeting throughout the PoP.	1	LO	NSP	NSP												
2001AJ	Bi-Annual PMR Minutes IAW paragraph 5.1.4.4 of the PWS. Due within five business days after the meeting.	2	EA	NSP	NSP												
2001AK	Ad-Hoc/Tiger Team Meeting Minutes IAW paragraph 5.1.4.5 of the PWS. Due one day prior to the next meeting or within five business days, whichever comes first.	1	LO	NSP	NSP												
2002	Cisco Base Services (SmartNet Total Care, Software Support Service, Business Critical Services) IAW PWS paragraphs 5.2, 5.3, 5.5, 5.6 and their subtasks. The annual Reconciliation/true-up IAW PWS 5.5.21.5 will establish the IB inventory and Lot Price for Option Period 2. Install Base Band (\$ Million): <table><tr><td>Install Base Bands (\$M)</td><td>Lot Price</td></tr><tr><td>500 - 600</td><td>\$</td></tr><tr><td>600 - 700</td><td>\$</td></tr><tr><td>700 - 800</td><td>\$</td></tr><tr><td>800 - 900</td><td>\$</td></tr><tr><td>900 - 1000</td><td>\$</td></tr></table>	Install Base Bands (\$M)	Lot Price	500 - 600	\$	600 - 700	\$	700 - 800	\$	800 - 900	\$	900 - 1000	\$	12	MO	\$	\$
Install Base Bands (\$M)	Lot Price																
500 - 600	\$																
600 - 700	\$																
700 - 800	\$																
800 - 900	\$																
900 - 1000	\$																

	<table><tr><td>1000 - 1100</td><td>\$</td></tr><tr><td>1100 - 1200</td><td>\$</td></tr><tr><td>1200 - 1350</td><td>\$</td></tr><tr><td>1350 - 1500</td><td>\$</td></tr></table> <p>PoP: 12 months from date of award.</p>	1000 - 1100	\$	1100 - 1200	\$	1200 - 1350	\$	1350 - 1500	\$						
1000 - 1100	\$														
1100 - 1200	\$														
1200 - 1350	\$														
1350 - 1500	\$														
2002AA	Mission Critical Device Listing IAW PWS paragraphs 5.2.3.1. Due within 48 hours of request from COR and on a 6-month basis.	1	LO	NSP	NSP										
2003	Cisco Software Support Services (SWSS) for Cisco Collaboration Edge and Unified SIP Proxy IAW PWS paragraph 5.3 and its subtasks. PoP: 12 months from exercise of option year. The Price for this CLIN shall be allocated to CLIN 1002.	12	MO	NSP	NSP										
2004	Cisco Collaboration Flex Enterprise Service IAW PWS paragraphs 5.4 and its subtasks. The annual Reconciliation/true-forward IAW PWS 5.5.21.6 will establish the price for Cisco Collaboration Flex Services in Option Period 2. Collaboration Flex Band (Knowledge Workers (KW)): <table><tr><td>Knowledge Workers (KW) Units Bands</td><td>Lot Price</td></tr><tr><td>260,000 - 311,999</td><td>\$</td></tr><tr><td>312,000 - 374,399</td><td>\$</td></tr><tr><td>374,400 - 449,279</td><td>\$</td></tr><tr><td>449,280 - 539,140</td><td>\$</td></tr></table> PoP: 12 months from exercise of option year.	Knowledge Workers (KW) Units Bands	Lot Price	260,000 - 311,999	\$	312,000 - 374,399	\$	374,400 - 449,279	\$	449,280 - 539,140	\$	12	MO	\$	\$
Knowledge Workers (KW) Units Bands	Lot Price														
260,000 - 311,999	\$														
312,000 - 374,399	\$														
374,400 - 449,279	\$														
449,280 - 539,140	\$														
2004AA	Collaboration Flex Enterprise Service Workspace IAW PWS paragraph 5.4.3. Due within 30 business days of exercise of option year.	1	LO	NSP	NSP										

2005	Cisco Business Critical Services IAW PWS Paragraphs 5.5 and its subtasks. PoP: 12 months from date of award. The Price for this CLIN and its SLINs shall be allocated to CLIN 1002.	12	MO	NSP	NSP
2005AA	Contractor/Network Consulting Engineering (NCE) Support Team Roster(s) IAW PWS paragraph 5.5.1 of the PWS. Due quarterly after exercise of option year.	1	LO	NSP	NSP
2005AB	Solution Delivery (SD) and Infrastructure Operations (IO) Documentation Reviews IAW PWS paragraph 5.5.5. Due within 10 business days of meeting.	1	LO	NSP	NSP
2005AC	Change Management Strategy Report IAW PWS paragraph 5.5.6. Due 180 days after award	1	LO	NSP	NSP
2005AD	Monthly Security Vulnerability/Common Services Platform Collector (CSPC) Report IAW PWS paragraph 5.5.7. Due monthly throughout the PoP.	12	MO	NSP	NSP
2005AE	Hosted Lab Test Cycles Solution Requirement Document (SRD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
2005AF	Hosted Lab Low Level Design Document (LLD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
2005AG	Hosted Lab Test Plan IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
2005AH	Hosted Lab Test Reports IAW PWS paragraph 5.5.8.	1	LO	NSP	NSP

	Due within 15 business days after testing is completed.				
2005AJ	Hosted Lab Status Reporting IAW PWS paragraph 5.5.8. Due monthly as part of CLIN 2001AC.	1	LO	NSP	NSP
2005AK	Routing and Switching Architecture Design Review Report IAW PWS paragraph 5.5.9.1. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
2005AL	Routing and Switching Stability Audit Report IAW PWS paragraph 5.5.9.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
2005AM	Routing and Switching Network Strategy Report IAW PWS paragraph 5.5.10. Due within 60 days of the topic being provided by VA.	4	EA	NSP	NSP
2005AN	Routing and Switching Consulting Sessions IAW PWS paragraph 5.5.10. The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
2005AP	Unified Communications (UC) Architecture Design Review Report IAW PWS paragraph 5.5.11.1. Due quarterly throughout the PoP.	1	LO	NSP	NSP
2005AQ	UC System Analysis Report IAW PWS paragraph 5.5.11.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
2005AR	UC Stability Audit Report IAW PWS paragraph 5.5.11.3.	1	LO	NSP	NSP

	Due within 60 days of the topic being provided by VA.				
2005AS	<p>UC Consulting Sessions IAW PWS paragraph 5.5.12.</p> <p>The Contractor shall deliver up to two strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
2005AT	<p>UC Infrastructure Strategy Roadmap Report IAW PWS paragraph 5.5.12 of the PWS.</p> <p>The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
2005AU	<p>Data Center/Unified Computing Architectural Assessment Plan (AAP) IAW PWS paragraph 5.5.13.1.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP
2005AV	<p>Data Center/Unified Computing Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	5	EA	NSP	NSP
2005AW	<p>Data Center/Unified Computing Consolidated Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP

2005AX	Data Center/Unified Computing Stability Audit Report IAW paragraph 5.5.13.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
2005AY	Data Center/Computing Infrastructure Strategy Roadmap Report IAW paragraph 5.5.14 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
2005AZ	Wireless LAN Architecture Design Review Report IAW paragraph 5.5.15.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
2005BA	Wireless LAN Stability Audit Report IAW paragraph 5.5.15.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
2005BB	Wireless LAN Network Infrastructure Strategy Roadmap Report IAW paragraph 5.5.16 of the PWS. Due within 60 days of the topic/location being provided by the VA.	4	EA	NSP	NSP
2005BC	Enterprise Video Teleconferencing Network (EVTN) Architecture/Stability Review Report IAW paragraph 5.5.17.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
2005BD	EVTN Business Video Strategy Roadmap Report IAW paragraph 5.5.18 of the PWS. Due within 60 days of the topic/location being provided by the VA	1	EA	NSP	NSP

2005BE	Common Services Platform Collector / Telepresence Management System Derived Improvement Report IAW paragraph 5.5.19.4 of the PWS Due within three (3) business days of request by VA, but no less than quarterly.	1	EA	NSP	NSP
2005BF	Cisco DNA Appliance Report IAW paragraph 5.5.19.5 of the PWS Due within 30 business days of award.	1	EA	NSP	NSP
2005BG	Monthly Knowledge Transfer Sessions IAW paragraph 5.5.20.1 of the PWS Due to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
2005BH	White Papers IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
2005BJ	Design Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
2005BK	Case Studies IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
2005BL	Support and Configuration Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal	1	LO	NSP	NSP

	posting and viewing by VA personnel, within 72 hours of creation and approval of the material.				
2005BM	Troubleshooting Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
2005BN	Deployment Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
2005BP	Training Documents IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
2005BQ	Cisco Learning Credits (CLCs) IAW paragraph 5.5.20.2 of the PWS The Government will authorize additional CLCs over and above the 5,125 CLCs provided with the install base price on an as-needed basis not to exceed 13,125 CLCs throughout the performance of the base period. At the conclusion of the base period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the base period. Initial base set of CLCs are due within 30 business days of award. Additional 2,000 CLC packs shall be delivered within 10 business days of request.	NTE 13,125	EA	\$	\$
2005BR	Cisco Platinum Learning Library Licenses IAW paragraph 5.5.20.4 of the PWS	200	EA	NSP	NSP

	Due within 30 business days of exercise of option year.				
2005BS	Annual Cisco Modeling Labs Licenses IAW paragraph 5.5.20.5 of the PWS Due within 30 business days of award or business days prior to end of license term period.	2	EA	NSP	NSP
2005BT	Install Base Inventory Database Report IAW paragraph 5.5.21.2 of the PWS Due Quarterly and final due within 60 days prior to the end of the PoP	1	LO	NSP	NSP
2005BU	Cisco Collaboration Flex Service Report IAW paragraph 5.5.21.3 Due Quarterly and final due within 60 days prior to the end of the PoP.	4	EA	NSP	NSP
2005BV	CBCESA User Access Report IAW paragraph 5.5.22 of the PWS. Due 180 days after award	1	LO	NSP	NSP
2006	CBCESA Prime Report and Subcontractor Reports IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract	1	EA	NSP	NSP
2006AA	CBCESA Service Organization Control Bridge Letter IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP
2007	ISO/IEC 27001 Certification IAW Addendum B, Section B4. Due annually	1	EA	NSP	NSP
TOTAL OPTION PERIOD TWO					\$

OPTION PERIOD THREE

This 12-month option may be exercised in accordance with 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 option period two.

Period of performance: October 1, 2021 through September 30, 2022

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
3001	<p>Program Management in accordance with (IAW) Performance Work Statement (PWS) 5.1.</p> <p>Period of performance (PoP) is 12 months from date of option exercise.</p> <p>The Price of this Contract Line Item Number (CLIN) and its Sub Contract Lin Item Numbers (SLIN) shall be allocated to CLINs 3002 and 3004</p>	12	MO	NSP	NSP
3001AA	<p>Contract Project Management Plan IAW paragraph 5.1.1 of the Performance Work Statement.</p> <p>The Contractor shall update and maintain and deliver the CPMP throughout the period of performance.</p>	1	LO	NSP	NSP
3001AB	<p>Contractor Staff Support Roster IAW paragraph 5.1.2 of the PWS.</p> <p>Due within five business days of a change or one business day prior to weekly Joint Program Management Office (JPMO) Meeting.</p>	1	LO	NSP	NSP
3001AC	<p>Cisco Business Critical Enterprise Service Agreement (CBCESA) Monthly Status Report IAW paragraph 5.1.3.1 of the PWS.</p> <p>Due monthly throughout the PoP. The CBCESA Monthly Status Report shall be delivered the last day of the preceding month.</p>	12	MO	NSP	NSP
3001AD	<p>CBCESA Service Level Agreement (SLA) Monitoring Plan IAW paragraph 5.1.3.2 of the PWS.</p> <p>Due within 15 business days of award and updated periodically thereafter.</p>	12	MO	NSP	NSP

3001AE	<p>CBCESA SLA Monitoring Report IAW paragraph 5.1.3.2 of the PWS.</p> <p>Due monthly after first 30 business days of award and updated periodically thereafter</p>	12	MO	NSP	NSP														
3001AF	<p>Technical Kickoff Meeting Minutes IAW paragraph 5.1.4.1 of the PWS.</p> <p>Due within five business days after the Kickoff Meeting.</p>	1	EA	NSP	NSP														
3001AG	<p>Weekly Joint Program Management Office JPMO Meeting Minutes IAW paragraph 5.1.4.2 of the PWS.</p> <p>Due one day prior to the next meeting or within three business days, whichever comes first.</p>	12	MO	NSP	NSP														
3001AJ	<p>Bi-Annual PMR Minutes IAW paragraph 5.1.4.4 of the PWS.</p> <p>Due within five business days after the meeting.</p>	2	EA	NSP	NSP														
3001AK	<p>Ad-Hoc/Tiger Team Meeting Minutes IAW paragraph 5.1.4.5 of the PWS.</p> <p>Due one day prior to the next meeting or within five business days, whichever comes first.</p>	1	LO	NSP	NSP														
3002	<p>Cisco Base Services (SmartNet Total Care, Software Support Service, Business Critical Services) IAW PWS paragraphs 5.2, 5.3, 5.5, 5.6 and their subtasks.</p> <p>The annual Reconciliation/true-up IAW PWS 5.5.21.5 will establish the IB inventory and Lot Price for Option Period 3.</p> <p>Install Base Band (\$ Million):</p> <table><tr><th>Install Base Bands (\$M)</th><th>Lot Price</th></tr><tr><td>500 - 600</td><td>\$</td></tr><tr><td>600 - 700</td><td>\$</td></tr><tr><td>700 - 800</td><td>\$</td></tr><tr><td>800 - 900</td><td>\$</td></tr><tr><td>900 - 1000</td><td>\$</td></tr><tr><td>1000 - 1100</td><td>\$</td></tr></table>	Install Base Bands (\$M)	Lot Price	500 - 600	\$	600 - 700	\$	700 - 800	\$	800 - 900	\$	900 - 1000	\$	1000 - 1100	\$	12	MO	\$	\$
Install Base Bands (\$M)	Lot Price																		
500 - 600	\$																		
600 - 700	\$																		
700 - 800	\$																		
800 - 900	\$																		
900 - 1000	\$																		
1000 - 1100	\$																		

	<table><tr><td>1100 - 1200</td><td>\$</td></tr><tr><td>1200 - 1350</td><td>\$</td></tr><tr><td>1350 - 1500</td><td>\$</td></tr></table>	1100 - 1200	\$	1200 - 1350	\$	1350 - 1500	\$								
1100 - 1200	\$														
1200 - 1350	\$														
1350 - 1500	\$														
	PoP: 12 months from date of award.														
3002AA	Mission Critical Device Listing IAW PWS paragraphs 5.2.3.1. Due within 48 hours of request from COR and on a 6-month period.	1	LO	NSP	NSP										
3003	Cisco Software Support Services (SWSS) for Cisco Collaboration Edge and Unified SIP Proxy IAW PWS paragraph 5.3 and its subtasks. PoP: 12 months from exercise of option year. The Price for this CLIN shall be allocated to CLIN 3002.	12	MO	NSP	NSP										
3004	Cisco Collaboration Flex Enterprise Service IAW PWS paragraphs 5.4 and its subtasks. The annual Reconciliation/true-forward IAW PWS 5.5.21.6 will establish the price for Cisco Collaboration Flex Services in Option Period 3. Collaboration Flex Band (Knowledge Workers (KW)): <table><tr><td>Knowledge Workers (KW) Units Bands</td><td>Lot Price</td></tr><tr><td>260,000 - 311,999</td><td>\$</td></tr><tr><td>312,000 - 374,399</td><td>\$</td></tr><tr><td>374,400 - 449,279</td><td>\$</td></tr><tr><td>449,280 - 539,140</td><td>\$</td></tr></table> PoP: 12 months from exercise of option year.	Knowledge Workers (KW) Units Bands	Lot Price	260,000 - 311,999	\$	312,000 - 374,399	\$	374,400 - 449,279	\$	449,280 - 539,140	\$	12	MO	\$	\$
Knowledge Workers (KW) Units Bands	Lot Price														
260,000 - 311,999	\$														
312,000 - 374,399	\$														
374,400 - 449,279	\$														
449,280 - 539,140	\$														
3004AA	Collaboration Flex Enterprise Service Workspace IAW PWS paragraph 5.4.3. Due within 30 business days of exercise of option year.	1	LO	NSP	NSP										
3005	Cisco Business Critical Services IAW PWS Paragraphs 5.5 and its subtasks.	12	MO	NSP	NSP										

	<p>PoP: 12 months from date of option year.</p> <p>The Price for this CLIN and its SLINs shall be allocated to CLIN 3002.</p>				
3005AA	<p>Contractor/Network Consulting Engineering (NCE) Support Team Roster(s) IAW PWS paragraph 5.5.1 of the PWS.</p> <p>Due quarterly after exercise of option year.</p>	1	LO	NSP	NSP
3005AB	<p>Solution Delivery (SD) and Infrastructure Operations (IO) Documentation Reviews IAW PWS paragraph 5.5.5.</p> <p>Due within 10 business days of meeting.</p>	1	LO	NSP	NSP
3005AC	<p>Change Management Strategy Report IAW PWS paragraph 5.5.6.</p> <p>Due 180 days after award</p>	1	LO	NSP	NSP
3005AD	<p>Monthly Security Vulnerability/Common Services Platform Collector (CSPC) Report</p> <p>IAW PWS paragraph 5.5.7.</p> <p>Due monthly throughout the PoP.</p>	12	MO	NSP	NSP
3005AE	<p>Hosted Lab Test Cycles Solution Requirement Document (SRD) IAW PWS paragraph 5.5.8.</p> <p>Due within 10 business days of VA request.</p>	1	LO	NSP	NSP
3005AF	<p>Hosted Lab Low Level Design Document (LLD) IAW PWS paragraph 5.5.8.</p> <p>Due within 10 business days of VA request.</p>	1	LO	NSP	NSP
3005AG	<p>Hosted Lab Test Plan IAW PWS paragraph 5.5.8.</p> <p>Due within 10 business days of VA request.</p>	1	LO	NSP	NSP

3005AH	Hosted Lab Test Reports IAW PWS paragraph 5.5.8. Due within 15 business days after testing is completed.	1	LO	NSP	NSP
3005AJ	Hosted Lab Status Reporting IAW PWS paragraph 5.5.8. Due monthly as part of CLIN 3001AC.	1	LO	NSP	NSP
3005AK	Routing and Switching Architecture Design Review Report IAW PWS paragraph 5.5.9.1. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
3005AL	Routing and Switching Stability Audit Report IAW PWS paragraph 5.5.9.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
3005AM	Routing and Switching Network Strategy Report IAW PWS paragraph 5.5.10. Due within 60 days of the topic being provided by VA.	4	EA	NSP	NSP
3005AN	Routing and Switching Consulting Sessions IAW PWS paragraph 5.5.10. The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
3005AP	Unified Communications (UC) Architecture Design Review Report IAW PWS paragraph 5.5.11.1. Due quarterly throughout the PoP.	1	LO	NSP	NSP
3005AQ	UC System Analysis Report IAW PWS paragraph 5.5.11.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
3005AR	UC Stability Audit Report IAW PWS paragraph 5.5.11.3.	1	LO	NSP	NSP

	Due within 60 days of the topic being provided by VA.				
3005AS	<p>UC Consulting Sessions IAW PWS paragraph 5.5.12.</p> <p>The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
3005AT	<p>UC Infrastructure Strategy Roadmap Report IAW PWS paragraph 5.5.12 of the PWS.</p> <p>The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.</p>	2	EA	NSP	NSP
3005AU	<p>Data Center/Unified Computing Architectural Assessment Plan (AAP) IAW PWS paragraph 5.5.13.1.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP
3005AV	<p>Data Center/Unified Computing Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	5	EA	NSP	NSP
3005AW	<p>Data Center/Unified Computing Consolidated Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.</p> <p>Due within 60 days of the topic/location being provided by the VA.</p>	1	EA	NSP	NSP

3005AX	Data Center/Unified Computing Stability Audit Report IAW paragraph 5.5.13.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
3005AY	Data Center/Computing Infrastructure Strategy Roadmap Report IAW paragraph 5.5.14 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
3005AZ	Wireless LAN Architecture Design Review Report IAW paragraph 5.5.15.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
3005BA	Wireless LAN Stability Audit Report IAW paragraph 5.5.15.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
3005BB	Wireless LAN Network Infrastructure Strategy Roadmap Report IAW paragraph 5.5.16 of the PWS. Due within 60 days of the topic/location being provided by the VA.	4	EA	NSP	NSP
3005BC	Enterprise Video Teleconferencing Network (EVTN) Architecture/Stability Review Report IAW paragraph 5.5.17.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
3005BD	EVTN Business Video Strategy Roadmap Report IAW paragraph 5.5.18 of the PWS. Due within 60 days of the topic/location being provided by the VA	1	EA	NSP	NSP

3005BE	Common Services Platform Collector / Telepresence Management System Derived Improvement Report IAW paragraph 5.5.19.4 of the PWS Due within three business days of request by VA, but no less than quarterly.	1	EA	NSP	NSP
3005BF	Cisco DNA Appliance Report IAW paragraph 5.5.19.5 of the PWS Due within 30 business days of award.	1	EA	NSP	NSP
3005BG	Monthly Knowledge Transfer Sessions IAW paragraph 5.5.20.1 of the PWS Due to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
3005BH	White Papers IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
3005BJ	Design Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
3005BK	Case Studies IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
3005BL	Support and Configuration Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel,	1	LO	NSP	NSP

	within 72 hours of creation and approval of the material.				
3005BM	<p>Troubleshooting Guides IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	1	LO	NSP	NSP
3005BN	<p>Deployment Guides IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	1	LO	NSP	NSP
3005BP	<p>Training Documents IAW paragraph 5.5.20.1 of the PWS</p> <p>Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.</p>	1	LO	NSP	NSP
3005BQ	<p>Cisco Learning Credits (CLCs) IAW paragraph 5.5.20.2 of the PWS</p> <p>The Government will authorize additional CLCs over and above the 5,125 CLCs provided with the install base price on an as-needed basis not to exceed 13,125 CLCs throughout the performance of the base period. At the conclusion of the base period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the base period.</p> <p>Initial base set of CLCs are due within 30 business days of award. Additional 2,000 CLC packs shall be delivered within 10 business days of request.</p>	NTE 13,125	EA	\$	\$
3005BR	Cisco Platinum Learning Library Licenses IAW paragraph 5.5.20.4 of the PWS	200	EA	NSP	NSP

	Due within 30 business days of exercise of option year.				
3005BS	Annual Cisco Modeling Labs Licenses IAW paragraph 5.5.20.5 of the PWS Due within 30 business days of award or business days prior to end of license term period.	2	EA	NSP	NSP
3005BT	Install Base Inventory Database Report IAW paragraph 5.5.21.2 of the PWS Due Quarterly and final due within 60 days prior to the end of the PoP	1	LO	NSP	NSP
3005BU	Cisco Collaboration Flex Service Report IAW paragraph 5.5.21.3 Due Quarterly and final due within 60 days prior to the end of the PoP.	4	EA	NSP	NSP
3005BV	CBCESA User Access Report IAW paragraph 5.5.22 of the PWS. Due 180 days after award	1	LO	NSP	NSP
3006	CBCESA Prime Report and Subcontractor Reports IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract	1	EA	NSP	NSP
3006AA	CBCESA Service Organization Control Bridge Letter IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP
3007	ISO/IEC 27001 Certification IAW Addendum B, Section B4. Due annually	1	EA	NSP	NSP
TOTAL OPTION PERIOD THREE					\$

OPTION PERIOD FOUR

This 12-month option may be exercised in accordance with 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 option period three..

Period of performance: October 1, 2022 through September 30, 2023

CLIN	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
4001	<p>Program Management in accordance with (IAW) Performance Work Statement (PWS) 5.1.</p> <p>Period of performance (PoP) is 12 months from date of option exercise.</p> <p>The Price of this Contract Line Item Number (CLIN) and its Sub Contract Lin Item Numbers (SLIN) shall be allocated to CLINs 4002 and 4004</p>	12	MO	NSP	NSP
4001AA	<p>Contract Project Management Plan IAW paragraph 5.1.1 of the Performance Work Statement.</p> <p>The Contractor shall update and maintain and deliver the CPMP throughout the period of performance.</p>	1	LO	NSP	NSP
4001AB	<p>Contractor Staff Support Roster IAW paragraph 5.1.2 of the PWS.</p> <p>Due within five business days of a change or one business day prior to weekly Joint Program Management Office (JPMO) Meeting.</p>	1	LO	NSP	NSP
4001AC	<p>Cisco Business Critical Enterprise Service Agreement (CBCESA) Monthly Status Report IAW paragraph 5.1.3.1 of the PWS.</p> <p>Due monthly throughout the PoP. The CBCESA Monthly Status Report shall be delivered the last day of the preceding month.</p>	12	MO	NSP	NSP
4001AD	<p>CBCESA Service Level Agreement (SLA) Monitoring Plan IAW paragraph 5.1.3.2 of the PWS.</p>	12	MO	NSP	NSP

	Due within 15 business days of award and updated periodically thereafter.														
4001AE	CBCESA SLA Monitoring Report IAW paragraph 5.1.3.2 of the PWS. Due monthly after first 30 business days of award and updated periodically thereafter	12	MO	NSP	NSP										
4001AF	Technical Kickoff Meeting Minutes IAW paragraph 5.1.4.1 of the PWS. Due within five business days after the Kickoff Meeting.	1	EA	NSP	NSP										
4001AG	Weekly Joint Program Management Office JPMO Meeting Minutes IAW paragraph 5.1.4.2 of the PWS. Due one day prior to the next meeting or within three business days, whichever comes first.	12	MO	NSP	NSP										
4001AJ	Bi-Annual PMR Minutes IAW paragraph 5.1.4.4 of the PWS. Due within five business days after the meeting.	2	EA	NSP	NSP										
4001AK	Ad-Hoc/Tiger Team Meeting Minutes IAW paragraph 5.1.4.5 of the PWS. Due one day prior to the next meeting or within five business days, whichever comes first.	1	LO	NSP	NSP										
4002	Cisco Base Services (SmartNet Total Care, Software Support Service, Business Critical Services) IAW PWS paragraphs 5.2, 5.3, 5.5, 5.6 and their subtasks. The annual Reconciliation/true-up IAW PWS 5.5.21.5 will establish the IB inventory and Lot Price for Option Period 4. Install Base Band (\$ Million): <table><tr><td>Install Base Bands (\$M)</td><td>Lot Price</td></tr><tr><td>500 - 600</td><td>\$</td></tr><tr><td>600 - 700</td><td>\$</td></tr><tr><td>700 - 800</td><td>\$</td></tr><tr><td>800 - 900</td><td>\$</td></tr></table>	Install Base Bands (\$M)	Lot Price	500 - 600	\$	600 - 700	\$	700 - 800	\$	800 - 900	\$	12	MO	\$	\$
Install Base Bands (\$M)	Lot Price														
500 - 600	\$														
600 - 700	\$														
700 - 800	\$														
800 - 900	\$														

	900 - 1000	\$													
	1000 - 1100	\$													
	1100 - 1200	\$													
	1200 - 1350	\$													
	1350 - 1500	\$													
	PoP: 12 months from date of award.														
4002AA	Mission Critical Device Listing IAW PWS paragraphs 5.2.3.1. Due within 48 hours of request from COR and on a 6-month basis.	1	LO	NSP	NSP										
4003	Cisco Software Support Services (SWSS) for Cisco Collaboration Edge and Unified SIP Proxy IAW PWS paragraph 5.3 and its subtasks. PoP: 12 months from exercise of option year. The Price for this CLIN shall be allocated to CLIN 4002.	12	MO	NSP	NSP										
4004	Cisco Collaboration Flex Enterprise Service IAW PWS paragraphs 5.4 and its subtasks. The annual Reconciliation/true-forward IAW PWS 5.5.21.6 will establish the price for Cisco Collaboration Flex Services in Option Period 4. Collaboration Flex Band (Knowledge Workers (KW)): <table><tr><th>Knowledge Workers (KW) Units Bands</th><th>Lot Price</th></tr><tr><td>260,000 - 311,999</td><td>\$</td></tr><tr><td>312,000 - 374,399</td><td>\$</td></tr><tr><td>374,400 - 449,279</td><td>\$</td></tr><tr><td>449,280 - 539,140</td><td>\$</td></tr></table> PoP: 12 months from exercise of option year.	Knowledge Workers (KW) Units Bands	Lot Price	260,000 - 311,999	\$	312,000 - 374,399	\$	374,400 - 449,279	\$	449,280 - 539,140	\$	12	MO	\$	\$
Knowledge Workers (KW) Units Bands	Lot Price														
260,000 - 311,999	\$														
312,000 - 374,399	\$														
374,400 - 449,279	\$														
449,280 - 539,140	\$														
4004AA	Collaboration Flex Enterprise Service Workspace IAW PWS paragraph 5.4.3. Due within 30 business days of exercise of option year.	1	LO	NSP	NSP										

4005	Cisco Business Critical Services IAW PWS Paragraphs 5.5 and its subtasks. PoP: 12 months from date of option year. The Price for this CLIN and its SLINs shall be allocated to CLIN 4002.	12	MO	NSP	NSP
4005AA	Contractor/Network Consulting Engineering (NCE) Support Team Roster(s) IAW PWS paragraph 5.5.1 of the PWS. Due quarterly after exercise of option year.	1	LO	NSP	NSP
4005AB	Solution Delivery (SD) and Infrastructure Operations (IO) Documentation Reviews IAW PWS paragraph 5.5.5. Due within 10 business days of meeting.	1	LO	NSP	NSP
4005AC	Change Management Strategy Report IAW PWS paragraph 5.5.6. Due 180 days after award	1	LO	NSP	NSP
4005AD	Monthly Security Vulnerability/Common Services Platform Collector (CSPC) Report IAW PWS paragraph 5.5.7. Due monthly throughout the PoP.	12	MO	NSP	NSP
4005AE	Hosted Lab Test Cycles Solution Requirement Document (SRD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
4005AF	Hosted Lab Low Level Design Document (LLD) IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP
4005AG	Hosted Lab Test Plan IAW PWS paragraph 5.5.8. Due within 10 business days of VA request.	1	LO	NSP	NSP

4005AH	Hosted Lab Test Reports IAW PWS paragraph 5.5.8. Due within 15 business days after testing is completed.	1	LO	NSP	NSP
4005AJ	Hosted Lab Status Reporting IAW PWS paragraph 5.5.8. Due monthly as part of CLIN 4001AC.	1	LO	NSP	NSP
4005AK	Routing and Switching Architecture Design Review Report IAW PWS paragraph 5.5.9.1. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
4005AL	Routing and Switching Stability Audit Report IAW PWS paragraph 5.5.9.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
4005AM	Routing and Switching Network Strategy Report IAW PWS paragraph 5.5.10. Due within 60 days of the topic being provided by VA.	4	EA	NSP	NSP
4005AN	Routing and Switching Consulting Sessions IAW PWS paragraph 5.5.10. The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
4005AP	Unified Communications (UC) Architecture Design Review Report IAW PWS paragraph 5.5.11.1. Due quarterly throughout the PoP.	1	LO	NSP	NSP
4005AQ	UC System Analysis Report IAW PWS paragraph 5.5.11.2. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP

4005AR	UC Stability Audit Report IAW PWS paragraph 5.5.11.3. Due within 60 days of the topic being provided by VA.	1	LO	NSP	NSP
4005AS	UC Consulting Sessions IAW PWS paragraph 5.5.12. The Contractor shall deliver up to two strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a VA Technology Program Managers (TPM) via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	2	EA	NSP	NSP
4005AT	UC Infrastructure Strategy Roadmap Report IAW PWS paragraph 5.5.12 of the PWS. The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.	2	EA	NSP	NSP
4005AU	Data Center/Unified Computing Architectural Assessment Plan (AAP) IAW PWS paragraph 5.5.13.1. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005AV	Data Center/Unified Computing Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	5	EA	NSP	NSP
4005AW	Data Center/Unified Computing Consolidated Architecture Design Review Report IAW paragraph 5.5.13.1 of the PWS.	1	EA	NSP	NSP

	Due within 60 days of the topic/location being provided by the VA.				
4005AX	Data Center/Unified Computing Stability Audit Report IAW paragraph 5.5.13.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005AY	Data Center/Computing Infrastructure Strategy Roadmap Report IAW paragraph 5.5.14 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005AZ	Wireless LAN Architecture Design Review Report IAW paragraph 5.5.15.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005BA	Wireless LAN Stability Audit Report IAW paragraph 5.5.15.2 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005BB	Wireless LAN Network Infrastructure Strategy Roadmap Report IAW paragraph 5.5.16 of the PWS. Due within 60 days of the topic/location being provided by the VA.	4	EA	NSP	NSP
4005BC	Enterprise Video Teleconferencing Network (EVTN) Architecture/Stability Review Report IAW paragraph 5.5.17.1 of the PWS. Due within 60 days of the topic/location being provided by the VA.	1	EA	NSP	NSP
4005BD	EVTN Business Video Strategy Roadmap Report IAW paragraph 5.5.18 of the PWS.	1	EA	NSP	NSP

	Due within 60 days of the topic/location being provided by the VA				
4005BE	Common Services Platform Collector / Telepresence Management System Derived Improvement Report IAW paragraph 5.5.19.4 of the PWS Due within three business days of request by VA, but no less than quarterly.	1	EA	NSP	NSP
4005BF	Cisco DNA Appliance Report IAW paragraph 5.5.19.5 of the PWS Due within 30 business days of award.	1	EA	NSP	NSP
4005BG	Monthly Knowledge Transfer Sessions IAW paragraph 5.5.20.1 of the PWS Due to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
4005BH	White Papers IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
4005BJ	Design Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
4005BK	Case Studies IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	EA	NSP	NSP
4005BL	Support and Configuration Guides IAW paragraph 5.5.20.1 of the PWS	1	LO	NSP	NSP

	Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.				
4005BM	Troubleshooting Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
4005BN	Deployment Guides IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
4005BP	Training Documents IAW paragraph 5.5.20.1 of the PWS Due as needed and submitted to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.	1	LO	NSP	NSP
4005BQ	Cisco Learning Credits (CLCs) IAW paragraph 5.5.20.2 of the PWS The Government will authorize additional CLCs over and above the 5,125 CLCs provided with the install base price on an as-needed basis not to exceed 13,125 CLCs throughout the performance of the base period. At the conclusion of the base period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the base period. Initial base set of CLCs are due within 30 business days of award. Additional 2,000 CLC packs shall be delivered within 10 business days of request.	NTE 13,125	EA	\$	\$

4005BR	Cisco Platinum Learning Library Licenses IAW paragraph 5.5.20.4 of the PWS Due within 30 business days of exercise of option year.	200	EA	NSP	NSP
4005BS	Annual Cisco Modeling Labs Licenses IAW paragraph 5.5.20.5 of the PWS Due within 30 business days of award or business days prior to end of license term period.	2	EA	NSP	NSP
4005BT	Install Base Inventory Database Report IAW paragraph 5.5.21.2 of the PWS Due Quarterly and final due within 60 days prior to the end of the PoP	1	LO	NSP	NSP
4005BU	Cisco Collaboration Flex Service Report IAW paragraph 5.5.21.3 Due Quarterly and final due within 60 days prior to the end of the PoP.	4	EA	NSP	NSP
4005BV	CBCESA User Access Report IAW paragraph 5.5.22 of the PWS. Due 180 days after award	1	LO	NSP	NSP
4006	CBCESA Prime Report and Subcontractor Reports IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract	1	EA	NSP	NSP
4006AA	CBCESA Service Organization Control Bridge Letter IAW paragraph 5.6.2 of the PWS. Due in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.	1	EA	NSP	NSP

4007	ISO/IEC 27001 Certification IAW Addendum B, Section B4. Due annually	1	EA	NSP	NSP
TOTAL OPTION PERIOD FOUR					\$

PRICING SUMMARY:

TOTAL BASE PERIOD:	\$
TOTAL OPTION PERIOD 1:	\$
TOTAL OPTION PERIOD 2:	\$
TOTAL OPTION PERIOD 3:	\$
TOTAL OPTION PERIOD 4:	\$
TOTAL PRICE:	\$

B.5 PERFORMANCE WORK STATEMENT



**PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology (OIT)
OIT IT Operations and Services (ITOPS)**

Cisco Business Critical Enterprise Service Agreement (CBCESA)

**Date: September 3, 2019
TAC-20-53098
PWS Version Number: 2.3**

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OIT), is to provide benefits and services to Veterans of the United States. In accomplishing the mission, OIT strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely, and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet its mission.

VA currently manages well over 525,000 Cisco networking, TelePresence, server, converged virtualization, and Unified Communications (UC) devices and applications that comprise the core of VA's IT infrastructure. These devices and applications require effective, proactive, on-going maintenance and support. In Fiscal Year (FY) 2015, VA established an enterprise-wide agreement to support these technologies. This contract seeks to continue and further modernize the vital services that provide branded Cisco Smart Net Total Care (SNTC) Service, Cisco Collaboration Flex Services, Cisco Software Support Services (SWSS), and Cisco Business Critical Services for VA OIT managed Cisco equipment and applications worldwide. The following paragraphs provide a general overview of these services. For the purposes of the PWS, these support capabilities collectively shall be referred to as the Cisco Business Critical Enterprise Service Agreement (CBCESA).

CISCO SMART NET TOTAL CARE SERVICE (SNTC)

SNTC is a proactive and reactive technical support service that provides VA staff with anytime access to Cisco engineers and Cisco.com resources to resolve critical issues related to Cisco Networking, Telephony, Unified Communications (UC), TelePresence, and Data Center/Unified Computing (server and converged virtualization) devices and applications. Cisco SNTC provides support for all covered devices, applications, and products including access to Cisco.com for online technical assistance; base Operating Systems(OS) software updates and support on devices and licensed operating system software, (including all maintenance, minor, and major releases); access to the Cisco Technical Assistance Center (TAC) 24 hours a day/seven days a week; equipment firmware updates, and advanced replacement of failed hardware either by next business day (8x5xNBD) or 24 hours a day/seven days a week/four hour delivery (24X7X4), depending on the type of equipment and its criticality to on-going operations.

CISCO SOFTWARE SUPPORT SERVICE (SWSS)

SWSS offers comprehensive coverage for software application products and suites. SWSS is a technical support offer for software that provides Cisco.com access, TAC support, and access to major and minor software upgrades for the covered product.

CISCO COLLABORATION FLEX SERVICES

Collaboration Flex provides cloud, on-premises, and hosted collaboration services and licensing in one unified service. Provides technical and operational support for meetings, messaging, and unified communications /calling services for VA Knowledge Workers (employees), to include software, upgrades, and support.

CISCO BUSINESS CRITICAL SERVICES:

Business Critical Services support the VA OIT mission by providing and supporting operational products and solutions currently in use while helping build an IT strategy for the future.

Business Critical Services are divided into three areas of support: Operations, Engineering, and Architecture.

Services for Operations provides capabilities and Deliverables in support of availability, security compliance, and management of Cisco infrastructure and application environment.

Services for Engineering provides capabilities and Deliverables in support of design and validation, application insights, threat analytics, automation, security programs, and hardening of Cisco infrastructure and application environment.

Services for Architecture provides capabilities and Deliverables in support of strategy, architecture alignment, design, deployment strategy, and adoption strategy for scaling of Cisco infrastructure and application environment.

Business Critical Services also include focused technical support, inventory management, knowledge transfers, mentoring, and training support (to include learning credits, lab testing, and modeling lab support).

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541-3549, “Federal Information Security Management Act (FISMA) of 2002”
2. “Federal Information Security Modernization Act of 2014”
3. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
7. 10 U.S.C. § 2224, “Defense Information Assurance Program”
8. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
9. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
12. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <http://www.va.gov/vapubs/>
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
14. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
15. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003

16. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
17. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, 2012
22. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
23. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, March 12, 2019
24. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring of VA Information Systems,” February 3, 2014
25. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle”, March 22, 2010
26. VA Handbook 6500.6, “Contract Security,” March 12, 2010
27. VA Handbook 6500.8, “Information System Contingency Planning”, April 6, 2011
28. OI&T Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
29. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)
30. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
31. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
32. VA Handbook 6510, “VA Identity and Access Management”, January 15, 2016
33. VA Directive 6300, Records and Information Management, February 26, 2009
34. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
35. NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 5, 2014
36. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
37. OMB Memorandum, “Transition to IPv6”, September 28, 2010
38. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
39. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
40. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
41. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
42. 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

43. 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
44. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
45. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
46. NIST SP 800-116 Rev 1, Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access, June 2018
47. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
48. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
49. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
50. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
51. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
52. 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>)
53. 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>))
54. VA Memorandum “Mandate to meet PIV Requirements for New and Existing Systems” (VAIQ# 7712300), June 30, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>
55. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.2, Federal Interagency Technical Reference Architectures, Department of Homeland Security, June 19, 2017, https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf
56. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
57. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
58. 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>)
59. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
60. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
61. Executive Order 13834, “Efficient Federal Operations”, dated May 17, 2018
62. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
63. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
64. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
65. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>

66. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
67. 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>
68. 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>
69. 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>
70. "Veteran Focused Integration Process (VIP) Guide 3.1", April 2018,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
71. "VIP Release Process Guide", Version 1.4, May 2016,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
72. "POLARIS User Guide", Version 1.9, March 2017,
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
73. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015,
<https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>

3.0 SCOPE OF WORK

The Contractor shall deliver Cisco branded SNTC Service and SWSS for VA OIT owned and managed Cisco equipment and applications worldwide to include all VA owned and managed Cisco brand Routing and Switching devices, Security systems, UC systems, Wireless Local Area Network (LAN) Systems, TelePresence, telephony, and Data Center/Unified Computing systems (servers and converged virtualization). SWSS services are limited to the systems as defined later in this PWS.

The Contactor shall deliver Cisco Collaboration Flex Enterprise Services to include cloud, on-premises, and hosted collaboration services and licensing in one unified service and shall provide technical and operational support for meetings, messaging, and unified communications /calling services for VA Knowledge Workers (employees), to include software, upgrades, and support as defined in this PWS.

The Contractor shall deliver Cisco Business Critical Services to support the VA OIT mission by providing and supporting operational products and solutions currently in use while helping build an IT strategy for the future to include optimization services to include focused technical support, inventory management, knowledge transfers, mentoring, and training support (to include learning credits, lab testing, and modeling lab support).

The Contractor shall deliver all services and support as defined in this PWS for all VA Administrations, Offices, and operational entities at the place of performance as defined in this PWS.

These collective unified support capabilities shall be referred to and constitute a CBCESA.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) shall be 12 months from date of award with four 12-month option periods.

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

All tasks under this PWS shall be provided to VA facilities throughout the world, with over 95% of all tasks estimated to be completed via remote support methods (collaborative tools, web-portals, etc.). Work may be performed at VA on-site locations with prior approval of the Contracting Officer's Representative (COR) and Primary Program Manager (PPM).

For a listing of all current VA facilities, use the VA facility listing drop-down menu found on the following VA web page: http://www.va.gov/directory/guide/rpt_fac_list.cfm?isflash=0

4.3 TRAVEL

The Government anticipates very limited travel under this effort to perform the tasks associated with the effort. Travel may, however, be required to attend program-related meetings or conferences throughout the period of performance. Travel costs will not be directly reimbursed by the Government and shall be included in the firm fixed price. The estimated amount of travel required under this CBCESA is approximately 5-10 visits per PoP and shall be coordinated with the VA COR and PPM.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROGRAM MANAGEMENT

5.1.1 CONTRACTOR PROGRAM MANAGEMENT PLAN

The Contractor shall deliver a Contractor Program Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of this contract. The CPMP shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be delivered within 10 business days of the award and concurred upon by the Government and updated in accordance with Section B of the Contract. The Contractor shall designate Contractor Program Manager and any additional support personnel they deem necessary and provide the contact information of each individual as part of the CPMP (this will be inclusive of any Cisco designated support personnel as defined in this PWS). The Contractor shall update and maintain and deliver the CPMP throughout the period of performance. The CPMP is at a minimum to be updated annually and at the start of each PoP and upon VA request during contract performance.

As part of the CPMP the following elements shall be included:

- A. Meeting Reviews – The Contractor shall provide a summary of all ongoing meetings, activities, and deliverables as defined in this PWS and their status.
- B. Project Management Support – Including Resource Allocation, Training, Personnel, and all other efforts necessary to facilitate contract activities.

Deliverable:

- A. Contractor Program Management Plan (CPMP)

5.1.2 JOINT PROGRAM MANAGEMENT OFFICE

Support and management oversight of this CBCESA shall be organized under a Joint Program Management Office (JPMO) that will coordinate general support activities, educational activities, and related support requirements. The JPMO shall consist of the VA COR, VA PPM, VA appointed Technology Program Managers (TPM), and key Contractor Management Team personnel. Contractor Management team may consist of any prime and sub-contracted support personnel. The Contractor shall provide and update as needed a Contractor Staff Support Roster. This roster shall also include all required elements as required in paragraph 6.2.2.

The initial Contractor Staff Support Roster shall be delivered to the COR and PPM within 10 business days of award. Changes to any assigned Contractor representatives on the JPMO shall be provided to the COR/PPM within five business days of change or one business day prior to any scheduled Weekly JPMO Meeting whichever is first.

The VA PPM in coordination with the CO, COR and TMPs may issue VA Standard Operating Procedures to support effective oversight and implementation of elements of this contract to which the Contractor shall be required to adhere.

Deliverable:

- A. Contractor Staff Support Roster

5.1.3 GENERAL REPORTING REQUIREMENTS

5.1.3.1 CBCESA MONTHLY STATUS REPORTING

The Contractor shall provide the COR and PPM with a written CBCESA Monthly Status Report in electronic form as defined in this PWS. Use of electronic deliverables and shared data portals is optional but encouraged. The report shall include detailed instructions and 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. All references in this PWS to “monthly” reporting requirements are inclusive of this report.

The CBCESA Monthly Status Report shall provide a detailed summary of all work completed during the reporting period and any work planned for the subsequent reporting period. The report shall identify any problems that arose during the period and a description of how the problem(s) were resolved to include any issues with meeting performance metrics and service level agreements as defined in this PWS. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor shall keep in communication with VA regularly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

After the technical kickoff meeting a draft report format and proposed content structure shall be provided and concurred on by the COR and PPM and or TPMs.

Deliverable:

- A. CBCESA Monthly Status Report

5.1.3.2 CBCESA SERVICE LEVEL AGREEMENT MONITORING PLAN AND REPORT

The Contractor shall provide an CBCESA Service Level Agreement (SLA) Monitoring Plan and Report that defines how SLA metrics will be monitored throughout the performance of the requirements in this PWS as well as a standard method to report.

The Contractor shall provide the initial SLA Monitoring Plan and Report to the COR and PPM for review and approval within 15 business days of award. Upon approval, the Contractor shall implement SLA monitoring in accordance with the approved plan and establish an SLA Dashboard that provides near real time SLA metrics data available to the VA. The Contractor shall provide the CBCESA SLA Report monthly which shall capture data as specified in the Deliverable Metrics/SLAs in this PWS (paragraph 6.4.1) with the initial report being due 30 business days after award. The CBCESA SLA Report shall be delivered in conjunction with the CBCESA Monthly Status Report. All SLAs in this PWS shall be reported monthly.

Deliverable:

- A. CBCESA SLA Monitoring Plan
- B. CBCESA SLA Monitoring Report

5.1.4 PROGRAM MEETINGS

5.1.4.1 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 business 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 for each effort. The Contractor shall propose dates, 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 Contracting Officer (CO), Contract Specialist (CS), COR and VA PPM. The Technical kickoff meeting may be held virtually or at a VA approved location. In addition, the Contractor shall provide all final Technical Kickoff meeting minutes within five business days after the Kickoff Meeting. The Contractor shall track and oversee all Technical Kickoff meeting follow-on items to closure. Tracking of these items will be included in the Weekly JPMO Meeting minutes until closed.

Deliverable:

A. Technical Kickoff Meeting Minutes

5.1.4.2 WEEKLY JOINT PROGRAM MANAGEMENT OFFICE MEETING

The Contractor shall conduct and manage virtual weekly JPMO meetings between the VA COR, PPM, TPMs, and Contractor staff. The Contractor (or its designated lead) shall discuss issues, track action items, discuss progress, review deliverables, and address any topics related to the services being provided under this contract. The Contractor shall deliver JPMO meeting minutes one day prior to the next scheduled meeting or within three business days, whichever comes first. The meeting minutes shall also include any Contractor documentation that was provided for and/or presented at the weekly meetings. Reporting format for these meeting minutes shall be coordinated and approved by the COR and PPM.

Deliverable:

A. Weekly JPMO meeting minutes

5.1.4.3 QUARTERLY STEERING COMMITTEE MEETING

The Contractor shall participate in a Quarterly Steering Committee (QSC) review, conducted virtually, with OIT ITOPS Solution Delivery (SD) and Infrastructure Operations (IO) leadership to brief on general progress and organizational priorities being supported under this contract. The QSC location will be announced at least 20 business days prior to the event and will be rotated at locations throughout VA. The QCS may be a mix of onsite and virtual attendees from both VA and the Contractor, with the participants primarily consisting of mid-level ITOPS leadership. Tasks accomplished by the Contractor's Cisco Business Critical Services team shall be reported and presented during this meeting. A draft report format and proposed content structure shall be provided and concurred on by the COR and PPM and or TPMs. All presentation slides/minutes shall be delivered at least four hours prior to any scheduled QSC.

Deliverable:

A. Steering Committee Slides/Minutes

5.1.4.4 BI-ANNUAL EXECUTIVE PROGRAM MANAGEMENT REVIEWS (PMR)

The Contractor shall participate in a bi-annual program management review that will be presented to VA senior IT leadership on the status of the overall CBCESA. The purpose of this

review is to provide VA senior IT leadership with a “snapshot” of the overall program, ongoing work efforts, meeting performance metrics and service level agreements and any VA designated topics. Contractor travel expenses shall be included in the firm-fixed price of this effort and will not be directly reimbursed to the Contractor. Within five business days after the meeting the Contractor shall provide meeting minutes that include topics covered, key issues/discussion points, actions and copies of all presentations. Coordination of this PMR shall be managed by the VA COR in conjunction with the PPM with Contractor support. Format and general content of this PMR briefing shall be provided by VA with guidance from VA senior IT leadership.

Deliverable:

- A. Bi-Annual PMR Minutes

5.1.4.5 AD HOC/TIGER TEAM MEETINGS

As determined by VA the Contractor shall support ad-hoc meetings, briefings and task specific tiger teams to meet unique or special requirements under this contract. Requests for this support presented to the Contractor by any VA IT staff member must be vetted and approved by the COR, PPM, and or TPM. The Contractor shall designate personnel to support and virtually attend meetings with VA representatives at a time and frequency as requested by the lead for the meeting or tiger team. Meetings will be documented, and meeting minutes published and copies to be provided to the VA COR, PPM, or appropriate TPM. The Contractor shall deliver the meeting minutes for any ad-hoc or tiger team meeting one day prior to the next meeting or within five business days, whichever comes first. Ad-hoc and Tiger Team efforts and progress will be reported during meetings of the JPMO, PMP, and QSC as directed by the COR or PPM.

Deliverable:

- A. Ad-Hoc/Tiger Team Meeting Minutes

5.2 CISCO SMART NET TOTAL CARE SERVICES

The Contractor shall deliver Cisco SNTC hardware and base operating system software support for 100 percent of VA’s owned inventory of Cisco hardware equipment and virtual systems (managed Cisco brand Routing and Switching devices, Security systems, UC systems, Wireless Local Area Network (LAN) Systems, TelePresence, telephony, and Data Center/Unified Computing systems (servers and converged virtualization).) as identified in Attachment 001 - VA Install Base (IB) and Attachment 002-VA Managed Cisco CSR 1000V Routers. This is a “services first” support capability, which stipulates that regardless of the current status of the device/systems entry status in the VA IB SNTC services and support will be provided without exception. The Contractor shall provide this Cisco support for all VA locations as defined in the Place of Performance and inclusive of all support as defined in paragraphs 5.2.1 to 5.2.8.

5.2.1 TECHNICAL ASSISTANCE CENTER

The Contractor shall provide unlimited, direct access to the Cisco TAC for technical support. The Contractor shall provide Cisco coverage 24 Hours x 7 Day x 365 Days per Year (24x7x365) via telephone, a web-based portal, e-mail, chat and social media for all hardware and software technical issues. The Contractor shall provide Cisco tracking and progress of the technical support being provided and shall report it as part of the Monthly Status Report. The Cisco TAC shall provide first call access to Cisco support directly to all authorized VA staff and partner contractor support members needing assistance on VA managed Cisco products. VA is the final authority as to whom to grant access to use these services. PWS paragraph 5.5.22 defines how access to use the services set forth in this agreement is granted and reviewed. The Cisco TAC

shall include assignment of a dedicated High-Touch Operations Manager (HTOM) as detailed in PWS paragraph Section 5.5.19.1.

All TAC cases will be opened using the standard severity levels as defined in the table below. Cases may be elevated from lower severity levels as needed to resolve or restore services at the request of VA or VA support personnel that initiated the original support case.

Severity Level	Definition	Standard Method to Open TAC Case
Severity 1 (S1)	When an existing network or environment is down or there is a critical effect on the end user's business operations.	<u>By phone:</u> Call Cisco TAC to open service request at 800-553-2447 Please note: For (S1) and (S2) requests, the customer must remain available for any communication attempts by the TAC engineer.
Severity 2 (S2)	When the operation of an existing network or environment is severely degraded or significant aspects of the end user's business operation are being negatively affected by unacceptable network performance.	<u>By phone:</u> Call Cisco TAC to open service request at 800-553-2447 Please note: For (S1) and (S2) requests, the customer must remain available for any communication attempts by the TAC engineer.
Severity 3 (S3)	When the operational performance of the network or environment is impaired, while most business operations remain functional.	<u>Via the Web:</u> Open service request using the online tool https://mycase.cloudapps.cisco.com/case By Phone: 800-553-2447
Severity 4 (S4)	When information is required about Cisco product capabilities, installation, or configuration and there is little or no effect on the end user's business operation	<u>Via the Web:</u> Open service request using the online tool https://mycase.cloudapps.cisco.com/case By Phone: 800-553-2447

DELIVERABLE METRICS/SLAs:

TAC Case Response: Cases opened at the Severity 1 and Severity 2 levels shall have a response time of 15 minutes or less for Severity 1 and 30 minutes or less for Severity 2. Cases opened at the Severity 3 and Severity 4 levels shall have a response time of 60 minutes or less for Severity 3 Service Events and NBD or less for Severity 4 Service Events. 95% of all TAC cases shall have a response time less than minimum acceptable performance level over a monthly cycle. The calculated metrics shall be provided in the CBCESA SLA Monitoring Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

TAC Case Restoration of Service: The restoration times for Severity 1 cases is four hours from notification and eight hours from notification for a Severity 2. The restoration times for Severity 3 cases is NBD or better. Severity 4 cases shall not have a restoration time. 95% of TAC cases shall have a restoration time less than minimum acceptable performance level over a monthly cycle. If the dispatch of a Return Material Authorization (RMA) or Field Engineer is required to

restore services, this SLA is not applicable. The calculated metrics shall be provided in the CBCESA SLA Monitoring Report, detailed logs of all ticket transactions shall be retained for the evaluation timeframe for audit if necessary.

5.2.2 CLASSIFIED NETWORK SERVICES-HIGH TOUCH TECHNICAL SERVICES (CNS-HTTS)

As a higher security alternate to the TAC, the Contractor will provide access to the Cisco Classified Network Services-High Touch Technical Services (CNS-HTTS) portal and services directly to all authorized VA staff and partner contractor support members needing assistance. Cases can be directly opened via a secure portal or via TAC with auto-rotation to the CNS based on device or system technology. CNS cases shall use the same severity levels, response times, and restoration requirements as general TAC cases (PWS paragraph 5.2.1) and will be reported as part of the CBCESA SLA Monitoring Report.

5.2.3 ADVANCED HARDWARE REPLACEMENT

The Contractor shall provide Cisco 8x5xNext Business Day Advanced Hardware Replacement (also known as Product Returns and Replacements (RMA)) for VA's installed base of Cisco devices except for devices designated as Mission Critical per PWS paragraph 5.2.3.1 which require that product returns and replacements be provided within four hours. The Contractor shall only provide new, or Cisco certified as equivalent to new, Cisco hardware of the same make and model as the replaced hardware. Factory seconds or remanufactured products are not acceptable. All replacement parts shall be manufactured by Cisco.

Absolutely no "Gray Market Goods" or "Counterfeit Electronic Parts" shall be provided under this process. Gray Market Goods are defined as genuine branded goods intentionally or unintentionally sold outside of an authorized sales-territory or by non-authorized dealers in an authorized territory. All equipment shall be accompanied by the Original Equipment Manufacturers (OEM) warranty. Counterfeit Electronic Parts are defined as unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

Any hardware product that must be returned for exchange under this process that contains either media or data/disk storage units must either be sanitized per VA-defined processes prior to return or the media or data/disk storage units shall be removed and retained by the VA for destruction. All other hardware, appliances, or systems less any media or data/disk storage units may be returned via the standard Cisco RMA process. VA will submit a Cisco Asset Destruction Approval Request Form as an administrative request prior to disposal of the media/data/disk unit. This will serve as final authorization to for the VA to dispose of the unit per VA sanitization procedures and is not revocable.

5.2.3.1 MISSION CRITICAL SUPPORT UPGRADE

VA shall identify for the Contractor specific devices/systems for mission critical support upgrade to the Cisco's 24x7x4 hour SNTC without additional cost. This upgrade shall be supported for up to and not to exceed 10 percent of most current VA's IB inventory count. VA will generally

identify these devices by serial number, chassis type, and physical location of the equipment with Mission Critical requirements, however, VA may designate an alternative means to target these to facilitate operations. Items marked as mission critical will be noted and tracked in the VA IB Inventory. The Contractor shall track and report metrics on the use of Cisco mission critical support and provide reports during the JPMO and in the Monthly report. These metrics shall be included in any presentation provided during the meeting and included in the meeting minutes.

The following table defines Cisco SNTC Replacement of Hardware and Onsite Field Engineer Delivery.

Level of Support	Description
8 X 5 X NBD	The Contractor shall deliver Cisco 8X5XNBD of replacement hardware for all equipment except mission critical devices. Advance replacement parts, without a field engineer, are delivered the next business day between 9 a.m. and 5 p.m. (provided the request is received before 3 p.m. local depot time).
24 X 7 X 4	<p>For mission critical devices, the Contractor shall deliver replacement hardware 24X7X4. 24 X 7 X 4 support includes onsite field engineering support if needed due to technical requirements of the issue and VA requests via the HTOM. Mission critical is defined as “any device, service, or system or non-redundant hardware whose failure or disruption results in the failure of business operations that have an immediate and enterprise level service disruption impact on patient care, benefits delivery or will cause a loss in funding to VA.”</p> <p>Enterprise level service disruptions are defined as:</p> <p>Service Disruption: a natural or man-made event that significantly disrupts the operational environment, such as damage to the organization’s building(s) and grounds due to severe weather, or an event that disrupts availability or access to a system, such as loss of utilities (power, telecommunications), accidents, or emergencies within the organization or in the surrounding community.</p> <p>Major Service Disruption: for the purposes of this document a major service disruption is defined as a service disruption to a critical system that impacts more than 100 users.</p> <p>Critical System: a system or application that based on VA expert judgment is essential to business line operations on a broad and continuous basis. The list of critical systems is contained in Attachment 1. This list will be updated periodically as new systems are deployed or business needs change. Mission critical equipment may include core switches, edge routers, and any other equipment/applications as determined by the VA, otherwise service is expected at the 8X5XNBD level. Examples</p>

Level of Support	Description
	of mission critical equipment include 3800s, 7200s, Aggregation Series Routers (ASRs), 6500s, Nexus series switches, and Video Communications Servers as indicated in the Cisco inventory.

The Contractor will at a minimum document, provide and support a semi-annual review of the current Mission Critical device listing. Additional reviews may be requested by the COR and PPM as needed. The Contractor shall make all updates to this list requested by VA within 48 hours of a formal request.

Deliverable:

- A. Mission Critical Device Listing

DELIVERABLE METRICS/SLAs:

Mission Critical Delivery: All TAC cases or RMA hardware replacement requests on systems or devices designated as mission critical shall ensure VA receipt at the VA provided delivery address of the replacement device, component, or system within a 4-hour window of time upon completion of all required RMA documentation.

The 95th percentile of Mission Critical Deliveries shall have a delivery time less than minimum acceptable performance level over a monthly cycle. The calculated metrics shall be provided in the CBCESA SLA Monitoring Report, detailed logs of all transactions shall be retained for the evaluation timeframe for audit if necessary

5.2.4 SOFTWARE DEVELOPERS

The Contractor shall provide direct access to Cisco software developers for critical VA issues (estimated at up to four sessions per PoP), related to Cisco only products, included in this contract. Engagement of access to Cisco Software Developers shall be made via the Contractor's Cisco Project Management Team, Cisco assigned Network Consulting Engineer (NCE), or the Cisco HTOM.

5.2.5 PRODUCT BUSINESS UNITS

The Contractor shall provide direct access to Cisco product Business Units (BU) for critical VA issues (estimated at up to four sessions per PoP), related to Cisco only products. Engagement of access to Cisco Product Business Units shall be made via the Contractors Cisco Project Management Team, Cisco assigned NCE, or the Cisco HTOM.

5.2.6 PRODUCTIVITY TOOLS AND SOFTWARE

The Contractor shall provide access to all Cisco sites for productivity tools and software support as listed below:

- A. Internet-enabled tools with firewall-friendly features; through secure, encrypted Java applets allow VA and Cisco engineers to work together more effectively.
- B. Details of new Cisco products and Cisco software.
- C. Information on patches and error notifications.
- D. SmartNet Total Care Portal (also known as Cisco Services Connection)
- E. Cisco Software Central (to include all license management capabilities-Traditional, SMART, and Enterprise Agreements)

- F. RMA Portal
- G. Any new portals or features developed over the life of this contract.

Access to the Smart Net Total Care Portal (also known as Cisco Services Connection) and Cisco Software Central (to include all license management capabilities-Traditional, SMART, and Enterprise Agreements) must be approved through the COR, PPM, or other VA designated administrators.

5.2.7 TROUBLESHOOTING TOOLS AND SUPPORT

The Contractor shall provide access to Cisco troubleshooting tools, Cisco support appropriate for knowledge expansion and problem diagnosis, to include:

- A. Interactive identification and troubleshooting of common hardware, configuration and performance issues.
- B. Informed decisions about which specific software version to use. The Contractor shall deliver to VA all proactive bug notifications based on VA network profile. These notifications shall inform VA of software bugs that could impact their network.
- C. Profile to receive email updates about reliability, safety, network security, and end-of-sale issues for the Cisco products specified.

All notifications, updates, upgrades, hardware replaced during the month shall be documented in the Monthly Status Report, discussed in Section 5.1.3.1.

5.3 CISCO SOFTWARE SUPPORT SERVICES (SWSS) FOR CISCO UNIFIED BORDER ELEMENT (CUBE)S AND CISCO® UNIFIED SESSION INITIATION PROTOCOL (SIP)

The Contractor shall deliver Premium Cisco SWSS for all current and future Cisco Unified Border Element (CUBE)s and Cisco® Unified Session Initiation Protocol (SIP) Proxy (CUSP)s. These products shall be considered part of the IB inventory for the purposes of this contract. This support will only be applicable to these products as they are not covered under the Cisco Collaboration Flex Enterprise Service as defined in paragraph 5.4 of this PWS. Premium Cisco Software Support Services entitles VA at a minimum to the following:

https://www.cisco.com/c/dam/en_us/about/doing_business/docs/cisco-software-support-service.pdf

The underlying host server for these applications shall be included in the IB inventory with a value equal to the host device and the value of the SWSS support. In the event Cisco changes its Premium Cisco Software Support Services during the period of performance of this contract, the Contractor agrees it will not provide services at a reduced level to what is currently maintained at the time of contract award.

5.3.1 CISCO CLOUD SERVICES ROUTER (CSR) 1000v SUPPORT

The Contractor shall provide the following support services for all VA managed CSRs to include any future procured instances. An initial list of all current VA CSR 1000Vs and assigned licenses will be provided as Attachment 2. Support shall include: Annual term renewals for all base, security and other licenses applied to VA managed CSRs for the base and any option periods. Licenses will be maintained and generated in the Cisco SmartNet Licensing Portal supporting

VA. Any new licenses feature or sets of features beyond this initial list must be procured by the VA prior to adding to this CBCESA for coverage.

Provide Enhanced SWSS for all VA managed CSRs to include all services as defined in this PWS to include paragraphs 5.2 through 5.3. SWSS coverage begins at award of these services and when new CSRs are procured by VA. CSRs are considered to be mission critical support as defined in PWS paragraph 5.2.3.1.

Annual reporting of supported CSR inventory will be as defined in paragraph 5.5.21.1 of this PWS.

5.3.2 SUPPORT EXCLUSIONS

Excluded from the list of supported software products/solutions under this contract are the following:

- a. All future Cisco acquisitions of products and services unless mutually agreed to by the Parties and incorporated into the IB.
- b. Cisco ONE / Cross-Catalog (xCAT) and any license and application support shall be negotiated and/or renewed outside of this contract

5.4 CISCO COLLABORATION FLEX ENTERPRISE SERVICE

The Contractor shall deliver Cisco Collaboration Flex Enterprise Services and support to VA for the following capabilities and quantities:

5.4.1 ENTERPRISE CALLING SERVICES

The Contractor shall deliver enterprise calling services to include access to Cisco hosted Private Branch Exchange (PBX) calling features as well as Webex, Webex Teams, Webex Hybrid Services, Cisco UC Manager, Cisco UC Communications Manager Session Management Edition (SME) Cisco Expressway Series (Core and Edge), Cisco Unity Connection, Soft Clients, Emergency Responder 911, Cisco Unified Survivable Remote Site Telephony (SRST), Cisco Unity Express, Cisco TelePresence Management Suite, Cisco Unified Communications IM and Presence (IM&P), Cisco Jabber and Cisco Unified Attendant Consoles. Webex services include features of meetings, events, training, and support.

All Webex and related Webex Teams services will be provided as Software as a Service (SaaS) and hosted in a Contractor provided via cloud hosted services that must be in a Federal Risk and Authorization Management Program authorized (FedRAMP) Moderate facility. These services must obtain an VA Authority to Operate (ATO) before operational use. Only the COR, PPM and assigned TPM shall have operational and management oversight of this capability.

Additional details on these Enterprise Calling Services capabilities are at:

<https://www.cisco.com/c/en/us/products/collateral/unified-communications/spark-flex-plan/datasheet-c78-740396.html>. Any service or support not defined in this PWS incorporates all elements as defined in the link above.

In the event Cisco changes these services during the period of performance of this contract, the Contractor agrees it will not provide services at a reduced level to what is currently maintained at the time of contract award.

Quantities of these services to be delivered are defined in paragraph 5.4.3.

5.4.2 ENTERPRISE CONTACT CENTER SERVICES

The Contractor shall deliver enterprise contact center services to include Premium capabilities to include browser-based agent desktop, inbound and outbound voice, call recording, touch-tone Interactive Voice Response (IVR), web and voice callbacks, and standard Customer Relationship Connectors (CMR), omnichannel communication such as chat and email, multi-channel reporting and analytics, and supervisor monitoring and barge-in for all types of agents. These services will be deployed at VA on-premise locations. Details on these Enterprise Contact Center Services capabilities are at:

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/OfferDescriptions/cisco_collaboration_flex_plan_contact_center.pdf. Any service or support not defined in this PWS incorporates all elements as defined in the link above.

In the event Cisco changes these services during the period of performance of this contract, the Contractor agrees it will not provide services at a reduced level to what is currently maintained at the time of contract award.

This service includes design support and operational support for the Cisco Unified Contact Center Enterprise (UCCE) platform. Due to the extensive enterprise support requirements of this platform and to deliver the specific skills, practices, and capabilities to the end user community above and beyond basic entry level product certifications the Contractor shall either have certification as an Advanced Technology Partner (ATP) for this platform or have access to a support vendor that has this same ATP certification for the duration of this effort.

5.4.3 CISCO COLLABORATION FLEX ENTERPRISE SUPPORT AND BASE REQUIREMENTS

The Contractor shall provide enhanced support services for all Enterprise Calling and Contact Center applications and services associated with this Cisco Collaboration Flex Enterprise Service plan inclusive of all services and software as described herein. All hosted Webex services shall have basic support. Flex Services includes on-premises licensing and software delivery via the existing VA Cisco hosted Smart Net Licensing Portal for all features inclusive of this service as an add-on element under Cisco Enterprise Agreement (EA) Workspace. The EA workspace for these services shall be active and available no later than 30 business days after award. Hardware support and services for telepresence devices are inclusive of this service.

Initial base capabilities for the VA Cisco Collaboration Flex Service are specified in the table below. During the contract period of performance, there will be growth, therefore, VA capabilities as set forth in the Table below represents VA capabilities at the time of contract award, and it is anticipated that such capabilities will grow and there is no cap on such growth.

Service Element	Initial Base VA Capabilities
Total Knowledge Workers	260,000
Total PBX Calling Users	260,000
Total Contact Center Concurrent Agents	Premium Concurrent Agents- 10,500 total
Total Active Meeting Hosts (will be 10% of KW count)	26,000
Meetings Audio Option	Meetings Toll Dial-In Audio or CCA-SP +VoIP

Included services based on service elements above	Factor
Common area	1 for every 5 KW, up to 50% total KW count
Essential licenses for analog devices and fax machines	1 for every 10 KW
TelePresence room	1 for every 100 KW
IP Phones Licenses	1.2 for every 1 KW
Unity Connection – Enhanced	1.2 for every 1 KW
Emergency Responder (e911)	1.2 for every 1 KW
Survivable Remote Site Telephony (SRST)	1 per KW
Communications Manager Express (CME)	1 for every 10 KW
Unity Express	1 for every 10 KW
Active Meeting Hosts	Meeting Center 1000 Event Center 1000 Training Center 1000 Support Center 5
10 Named Users	Event Center 3000
Webex Teams	Messaging, file sharing, white boarding, video, calling. Webex Teams file storage – 20GB per KW
Webex Hybrid Services	Hybrid Call Service, Calendar Service, Directory Service, Video Mesh, and Data Security Service. Hybrid Call Service integrate VA call control with Cisco Webex Teams and Cisco Webex Meetings. Video Mesh Service, Webex meeting engine on-premises to provide local media processing for on-premises video quality and optimized Internet bandwidth.
Cloud Device registration	Webex Room and Desk Devices for DX series, DX70, DX80, MX series, MX200 G2, MX300 G2, MX700 (all), MX800 (all), SX series, SX10, SX20, SX80, Webex Codec Plus, Webex Quad Camera, Webex Room 50, Webex Room 55, Webex Room 55 Dual, Webex Room 70, Webex Room 70 G2, Webex Room Kit, Webex Room Kit P60, Webex Room Kit Plus & Pro Whiteboarding and Mark Up Connectivity and Sharing from Webex Team application

Inventory and adjustment of this service will be as defined in paragraph 5.5.21.9 of this PWS. “Knowledge Workers” are VA employees and VA contractors who use computing or communications devices capable of running the Cloud Services and using the Software as defined in this PWS as part of their job duties. Knowledge Worker count also includes the employees of any VA affiliates that may use these services as part of engagement with the VA.

“VA affiliates” are affiliated institutions that may include but are not limited to academic institutions and other sponsoring institutions such as community hospitals, clinics, state agencies military treatment facilities, tribal governments, or Federal Health Education Consortia. The VA must have a written agreement with any such entity.

A “Meeting” is a meeting initiated: (a) in Webex Meetings, Webex Teams, or Cisco Meeting Server; or (b) by phone using a Webex personal conferencing number regardless of whether Webex Meetings, Webex Teams, or Cisco Meeting Server is launched as part of the Enterprise Calling Services.

“Concurrent Agent” means the maximum quantity of Contact Center Users that are simultaneously logged-in to use the Collaboration Flex Plan Contact Center software or services.

“Active Meeting Hosts” are Knowledge Workers that access the Cisco software and cloud services and that host at least one meeting.

Deliverable(s):

- A. Cisco Collaboration Flex Enterprise Services
- B. Collaboration Flex Enterprise Service Workspace

5.5 CISCO BUSINESS CRITICAL SERVICES

5.5.1 CISCO OPTIMIZATION SERVICES

The Contractor shall deliver the following Cisco Optimization Support Services under the business-critical services: Routing & Switching, UC, Datacenter/Unified Computing, Wireless LANs, and TelePresence (Business Video) Systems.

The Contractor shall support these optimization support services to include appropriate Network Consulting Engineering (NCE) support teams of personnel for the above listed systems/technology areas. Optimization support shall notify VA of Cisco best practices, where VA could improve its environment by suggesting changes to the environment that would improve overall performance, standardize and rationalize equipment, and/or decrease costs. This will be provided through the various deliverable reports required for each technology area as noted in this PWS.

The Contractor will provide the COR and PPM with a report of all Contractor supporting NCE team personnel to include all assigned program managers and support staff. This report will provide the Contractor support staff and NCE team members name, work e-mail, business contact number, and assigned technology area. The format of this report shall be agreed upon by the Contractor, COR, and PPM. This report shall be updated at a minimum on a quarterly basis unless updates are required due to personnel changes.

Deliverable:

A. Contractor/NCE Support Team Roster(s)

5.5.2 OPTIMIZATION ENGINEERING SUPPORT

The Contractor shall deliver all Cisco Business Critical and optimization engineering support specified under this PWS to VA ITOPS IO and SD. All software, hardware, design, change, management efforts must comply with applicable Federal, One-VA architecture, VA Technical Reference Model (VA TRM), and SD approved baseline configurations.

The Contractor shall support and use the Cisco Common Services Platform Collector (CSPC) platform (paragraph 5.5.19.4) to help identify deficiencies and potential risks that should be resolved to optimize availability, stability, and performance of VA's Cisco infrastructure and application environment. Optimization engineering support also helps assess the effectiveness of the Cisco environment for purposes of planning current and future changes based on VA's evolving business imperatives and requirements.

The CSPC provides the following reports via the SmartNet Portal: Best Practices, Hardware Lifecycle Milestones, Diagnostic Analysis, Platform Insights, Field Notices (where applicable) and Audits. These are accessible via the Cisco Smart Net Total Care Portal. This platform can be used for ad-hoc reporting or in support of any of the Business-Critical Insights optimization services in this PWS.

5.5.3 SOFTWARE STRATEGY

The Contractor shall deliver Cisco's monthly Six-Sigma reporting as an appendix to the Monthly Status Report on conformance of VA's Cisco assets to the SD published baseline configuration for the components and report on how the SD baselines align with the latest Cisco recommendations for software for the Cisco components in question. Software conformance reporting shall use data extracted from the Cisco CSPC. These reports shall be designed to ensure that VA effectively manages the software lifecycle while improving consistency, standardization, availability and performance. The Contractor may also participate in and support joint discussions with VA on VA's overall software strategy to include the development of operating procedures and support documentation. These work efforts will be reported as part of the Monthly Status Report and other business meetings as determined by the COR and PPM.

5.5.4 HARDWARE STRATEGY

Monthly, utilizing CSPC and TelePresence Management Suite (TMS) data and feedback from meetings, technical support cases, or onsite visits the prior month, the Contractor shall deliver Cisco's proactive identification of VA issues that could affect performance and stability of any Cisco devices or configurations within the environment. The Contractor shall provide Cisco's remediation strategies to minimize the risk associated with the identified issues. The issues identified shall be reported to the respective IO Infrastructure Service Line Manager and SD. Any critical issues shall be included as part of the Monthly Status Report to provide visibility for senior management and attention to this matter.

5.5.5 DESIGN STRATEGY

Upon request by SD or an IO Service Line Manager and through the COR and PPM or TPM, the Contractor shall deliver Cisco's design consultation services in support of VA's efforts to maintain, evolve and align with current and future design standards for Cisco hardware. The

Contractor shall deliver Cisco's support on these ad hoc design consultations (estimated at one per quarter) when environmental changes, new facilities, or changes in OIT strategies dictate a particular network redesign. Design strategies shall follow Cisco's most up-to-date recommendations for hardware and software configurations at the time of being provided. Design strategies shall follow SD published baseline configurations and the Contractor shall deliver a copy of all design consultations to SD for review prior to submission to IO operations staff. Where the Contractor recommendations differ from published SD published baseline configurations the Contractor shall highlight for VA and indicate why they feel deviation is recommended.

Any written comments resulting from project-based requests for design consultation shall be provided to SD, first for review, prior to submission to the requesting region to ensure that SD approved standards are being followed in the recommendations. The Contractor shall deliver Cisco's documentation review of SD/IO documentation. The Contractor shall provide Cisco's comments within five business days of request.

Deliverable:

- A. SD/IO Documentation Reviews

5.5.6 CHANGE MANAGEMENT STRATEGY

The Contractor shall deliver Cisco's annual review of VA's change management strategies with respect to networking, UC, Unified Computing, and TelePresence equipment, to include recommendations as to how VA's strategies can be improved. Specific attention shall be paid to new Cisco technologies and how they require modernization or process flow changes, with respect to existing methodologies used by VA to ensure maximum value of the new technology. This report shall be delivered at the 180-day point of each PoP.

Deliverable:

- A. Change Management Strategy Report

5.5.7 SECURITY VULNERABILITY REPORTING

Due to the critical nature of security vulnerabilities and their potential impact on VA operations and protection of our Veteran's data, the Contractor shall proactively notify VA when Critical and High security vulnerabilities are identified that affect current installed inventory of devices or systems. Initial reporting of all newly identified Critical and High security vulnerabilities as identified by the Cisco Product Security Incident Response Team (PSIRT) (e.g., security advisories, responses, and notices) shall be delivered by the Contractor to VA in Security Vulnerability Reports, within one standard business day of Cisco's initial public release using a standard VA approved e-mail template. This serves as an initial notice of the potential issue only and not a solution unless one is available at the time of publication. Medium/Low and informational advisories will be the responsibility of the VA team to review via the Cisco support website as well as subscribed e-mail alerts and additional information as requested from the Cisco Network Consulting Teams. Prior to generating a report all security vulnerabilities identified by PSIRT shall be compared to current CSPC/TMS database of devices covered under this PWS before being sent to VA so that only vulnerabilities that could possibly impact VA are reported.

A report including all vulnerability announcements released during a given month shall be sent to VA by the second week of the following month. This monthly report will be accompanied by

a CSPC/Total Care report identifying all currently open vulnerabilities impacting VA along with the detailed device information.

After the initial report is provided to VA, any modification or update to the Critical and High vulnerability shall be delivered to VA using the agreed upon template via Email and also within one standard business day of Cisco's update release. As part of the initial and any follow-on reporting the Contractor shall provide Cisco's security alert remediation strategies, code recommendations and software/operating system multi-generational plans. The Contractor shall detail in the report additional information that describes the specific impact to VA hardware, software, configuration, applications, software strategy, and any specific remediation recommendations. Cisco's recommended strategies, other recommendations and plans shall also be documented and tracked in the Monthly Reports in addition to the Monthly Security Vulnerability/CSPC Report.

Deliverable:

- A. Monthly Security Vulnerability/CSPC Report

5.5.8 HOSTED LAB TEST CYCLES

The Contractor shall provide a Cisco Hosted Lab Test Environment to support testing and validation of new technical, software, security, operational standards for all Cisco hardware networking devices, telephony, TelePresence, UC, and Unified Computing (servers and converged virtualization) devices and applications supported under this PWS. This hosted lab shall mirror/simulate the overall VA enterprise and be updated throughout its life cycle. Lab support engagements must be formally requested and approved by a joint VA and Contractor team to include overall prioritization of lab efforts. The overall process of Lab engagements will follow this cycle:

- A. Test lab administration support
- B. Test tool use and support
- C. Physical environmental lab footprint
- D. Testing Process
 - a. Assessment
 - b. Planning
 - c. Setup
 - d. Execution
 - e. Results
- E. Detailed reports

The details of the specific engagements shall be agreed upon in writing by VA and the Contractor at least two weeks prior to the Test as a Service (TAAS). Design, engineering, testing, training and remote support. TAAS is focused on hardware and software lifecycles projects and will take a solution to pilot using an independent verification and validation lab. The lab will use test-proven and refined architecture to produce validated configurations, which are delivered to customers through a hands-on knowledge transfer. Each new solution remains in a semi-static test bed allowing problems to be solved in the lab and solutions to be rapidly deployed. This method of procedure produces a System/Solution Requirement Document (SRD), Low Level Design Document (LLD), Test plan, and written Test report. Training shall be provided before and after the engagement. Testing will be conducted on existing systems and new systems to facilitate a transition from legacy to next generation technologies. VA personnel

may participate in the testing cycle remotely or on site at VA's discretion. VA personnel will have constant access to Contractor Test personnel and information. Access to equipment will be accomplished through a request process to allow for scheduling and quick restoration to standard configurations.

The Contractor shall provide periodic reports on the current status of the hosted lab to include; tracking of ongoing requests, tracking of any hosted lab updates, upgrades, ore changes, and any outages. Lab status and usage will be part of the monthly status report.

Deliverables:

- A. Hosted Lab SRD
- B. Hosted Lab LLD
- C. Hosted Lab Test Plan
- D. Hosted Lab Test Reports
- E. Hosted Lab Status Reporting

5.5.9 ROUTING & SWITCHING OPTIMIZATION SERVICE

The Contractor shall provide Cisco's Routing and Switching Optimization Service in support of the VA Enterprise Routing and Switching Network Infrastructure. Contractor support shall consist of the following individual service elements:

5.5.9.1 ARCHITECTURE DESIGN REVIEW

The Contractor shall provide four Architecture Design Reviews per PoP. VA will provide Routing and Switching Network topics 60 days prior to the design reviews.

The Contractor shall deliver Architecture Design Review Reports utilizing Cisco standard practices covering Routing and Switching Network architecture assessments and elements. This report shall be due within 60 days of the topic being provided by the VA.

Deliverable:

- A. Routing and Switching Architecture Design Review Report

5.5.9.2 STABILITY AUDIT

The Contractor shall provide and deliver four stability audits per PoP for the following items for Routing and Switching Network:

- A. Network Improvement Plan
- B. Hardware Field Notice Report
- C. Technology Audit
- D. Hardware End-of-Life (EoL) report
- E. Hardware Service report
- F. Custom configuration report
- G. Configuration Best Practices report
- H. Software infrastructure and security report
- I. System log analysis report

The Contractor shall deliver Stability Audit Reports utilizing Cisco standard practices covering network performance assessments. The use of web tools, dashboards, and other online applications in support of this requirement is required. These reports shall be due within 60 days of the topic being provided by the VA.

Deliverable:

- A. Routing and Switching Stability Audit Report

5.5.10 BUSINESS ROUTING AND SWITCHING STRATEGY CONSULTING

The Contractor shall provide and deliver four Business Routing and Switching Network Strategy reports per PoP for the following items for the Routing and Switching Network:

- A. Analysis of current and planned projects
- B. Development of Return on Investment (ROI) models
- C. Use case analysis and mapping to projects

The Contractor shall deliver Business Routing and Switching Network Strategy Reports utilizing Cisco standard practices covering business Routing and Switching deployments. The use of web tools, dashboards, and other online applications in support of this report is required.

The Contractor shall deliver up to three strategy consulting sessions annually not to exceed four hours in length per session on a topic requested by a TPM via the COR to include remote lab access. These reports shall be due within 60 days of the topic being provided by the VA.

Deliverable:

- A. Routing and Switching Network Strategy Report
- B. Routing and Switching Consulting Sessions

5.5.11 UNIFIED COMMUNICATIONS OPTIMIZATION SERVICE

The Contractor shall provide UC Optimization Service in support of the VA Enterprise UC Infrastructure. For the purposes of this PWS UC is inclusive of all Cisco Contact Center Applications regardless of deployment method. Contractor support shall consist of the following individual service elements:

5.5.11.1 ARCHITECTURE DESIGN REVIEW

The Contractor shall deliver one annual Architecture Design Review (ADR) per PoP covering the following topics in support of the Unified Communication Infrastructure:

- A. Consult with VA designated TPM in a series of meetings to develop a thorough understanding of VA's UC design requirements, impacting the UC system, with a focus on resiliency, self-recovery, scalability, and ability to handle increased traffic demands and Quality of Service (QoS).
- B. The Contractor shall provide Cisco's recommendations on UC to include the following:
 1. Review of VA's UC requirements, priorities, and goals.
 2. Analysis of impact of new requirements on existing UC system.
 3. Review of Network Infrastructure architecture and topology impacting the UC system.
 4. Review of voice protocol selection and configuration.
 5. Review of UC feature selection.
 6. Review of UC system configuration.

7. Review of security considerations (i.e., authentication, VLANs, subnet isolations).
8. Provide report describing design review and recommendations.

The Contractor shall deliver an UC Architecture Design Review Report on the detailed design utilizing Cisco standard practices covering Unified Communication Infrastructure architecture and shall address: recommended additions or changes related to dial plan, Call Manager cluster design, UC system redundancy, gateways, gatekeepers and Call Manager configuration recommendations and any applicable test procedures for changes to the Network. This report shall be due within 60 days of the topic being provided by the VA.

Deliverable:

- A. UC Architecture Design Review Report

5.5.11.2 SYSTEM ANALYSIS

The Contractor shall provide one annual UC Design Support Service to evaluate VA's existing UC strategy based on published best practices and industry standards. This service shall evaluate serviceability, scalability, and security components as well as the infrastructure and practices used to deploy a UC solution.

- A. Network Infrastructure for Voice and Video over IP (e.g., inline power, QoS)
- B. Network services (e.g., Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP))
- C. Network links (e.g., LAN, WAN)
- D. Hardware / Software compliance
- E. Cisco Call Manager (clustering, failover/redundancy)
- F. Dial plan / Call routing
- G. Media resources
- H. Voice mail / PBX integration
- I. UC security best practices
- J. Directory integration (e.g., external directories such as Active Directory or Netscape)
- K. Service fine tuning
- L. Cisco application integration with Communications Manager (e.g., Cisco Emergency Responder, Personal Attendant)

This report shall be due within 60 days of the topic being provided by the VA.

Deliverable:

- A. UC System Analysis Report

5.5.11.3 STABILITY AUDIT

The Contractor shall provide one annual stability audit per PoP for the following items for UC Infrastructure:

- A. Network Improvement Plan
- B. Hardware Field Notice Report
- C. Technology Audit
- D. Hardware Service report
- E. Custom configuration report
- F. Configuration Best Practices report

- G. Software Improvement Plan
- H. Software infrastructure and security report
- I. System log analysis report

The Contractor shall deliver a Stability Audit Report utilizing Cisco standard practices covering network performance assessments. The use of web tools, dashboards, and other online applications in support of this requirement is required. This report shall be due within 60 days of the topic being provided by VA

Deliverable:

- A. UC Stability Audit Report

5.5.12 BUSINESS UNIFIED COMMUNICATION CONSULTING

The Contractor shall provide one Business UC Infrastructure Strategy Roadmap report per PoP for the following items for the UC Infrastructure:

- A. Analysis of current and planned projects
- B. Development of ROI models
- C. Use case analysis and mapping to projects

The Contractor shall deliver a UC Infrastructure Strategy Roadmap Report utilizing Cisco standard practices covering UC Infrastructure deployments. The use of web tools, dashboards, and other online applications in support of this report is required.

The Contractor shall deliver up to two UC Consulting sessions annually not to exceed four hours in length per consulting session on a topic requested by the TPM to include remote lab access. These reports shall be due within 60 days of the topic being provided by VA.

Deliverable:

- A. UC Infrastructure Strategy Roadmap Report
- B. UC Consulting Sessions

5.5.13 DATA CENTER/UNIFIED COMPUTING OPTIMIZATION SERVICE

The Contractor shall provide Cisco Data Center/Unified Computing Optimization Service in support of the VA Enterprise Data Center/Unified Computing Infrastructure. Contractor support shall consist of the following individual service elements.

5.5.13.1 ARCHITECTURE DESIGN REVIEW (ADR)

VA consists of multiple levels of facilities that support our mission which over time can lead to reduced efficiency and drifting from standards. The Contractor shall conduct ADR at VA selected locations. These ADRs will provide local administrators information to improve efficiency as well as corrective guidance to avoid device or network failures. In addition, the ADRs shall provide SD a view into local infrastructure, insights to develop national policy, assist in training recommendations, and develop new strategies.

The Contractor shall also deliver prior to and as part of the ADR process an Architecture Assessment Plan (AAP) which will identify the following items:

1. Strategy for conducting a site assessment including the devices that will be analyzed.

2. Points of analysis, such as network topology, hardware platform, hardware/software protocols, addressing and routing strategy, scalability, redundancy, security considerations.
3. Level of effort expected from VA employees.
4. Schedule for achieving yearly objectives including site audit, analysis, and ADR delivery schedule.

The Contractor shall provide one ADR per site type using the approved AAP, for each PoP. The site types and quantities are identified below:

1. One Enterprise WAN
2. One Enterprise Data Center
3. Two Regional Data Centers
4. Two Hospital Data Centers
5. Four Field Sites (Outpatient Clinics)

The Contractor shall provide a Consolidated ADR Report for the site types listed. The Consolidated ADR shall contain the information gathered from each site as well as a consolidated analysis of information obtained:

- A. System log analysis report
- B. Technology Audit
- C. Hardware Field Notice Report
- D. Software infrastructure and security report
- E. Hardware Service report
- F. Custom configuration report
- G. Configuration Best Practices report

The Contractor shall coordinate the elements of the Consolidated ADR with the COR and SD to further refine the ADR process and output. The Contractor shall deliver the AAP, Data Center/Unified Computing ADR Report, and Consolidated ADR Report utilizing Cisco standard practices covering Cisco Data Center/Computing Infrastructure architecture assessments and elements. These reports shall be due within 60 days of the locations being provided by VA.

Deliverables:

- A. Data Center/Unified Computing AAP
- B. Data Center/Unified Computing ADR Report
- C. Data Center/Unified Computing Consolidated ADR Report

5.5.13.2 STABILITY AUDIT

The Contractor shall provide one annual stability audit per PoP for the following items for Cisco Data Center/Computing Infrastructure:

- A. Network Improvement Plan
- B. Software Improvement Plan

The Contractor shall deliver Cisco's Stability Audit Report utilizing Cisco standard practices covering network performance assessments. The use of web tools, dashboards, and other online

applications in support of this requirement is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. Data Center/Unified Computing Stability Audit Report

5.5.14 BUSINESS CISCO DATA CENTER/COMPUTING CONSULTING

The Contractor shall provide one Business Cisco Data Center/Computing Infrastructure Strategy Roadmap report per PoP for the following items for the Cisco Data Center/Computing Infrastructure:

- A. Analysis of current and planned projects
- B. Development of ROI models
- C. Use case analysis and mapping to projects

The Contractor shall deliver a Data Center/Computing Infrastructure Strategy Roadmap Report utilizing Cisco standard practices covering Data Center/Computing Infrastructure deployments. The use of web tools, dashboards, and other online applications in support of this report is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. Data Center/Computing Infrastructure Strategy Roadmap Report

5.5.15 WIRELESS LANS OPTIMIZATION SERVICE

The Contractor shall provide Cisco Wireless LAN Optimization Service in support of the VA Enterprise Wireless LAN Network. Contractor support shall consist of the following individual service elements:

5.5.15.1 ARCHITECTURE DESIGN REVIEW

The Contractor shall provide one Architecture Design Review per PoP covering the following topics/elements in support of the VA Wireless LAN Network:

- A. Review design requirements, priorities, and goals by comparing business direction and feature/functionality requirements against current VA SD baselines for enterprise wireless networking. Review will identify key functionality gaps between these elements.
- B. Include recommendations for architectural changes, security enhancements, performance improvements, system changes, and/or application migration.
- C. Review VA wireless LAN business goals, objectives, and requirements against best business practices and SD wireless baselines
- D. Review existing VA wireless LAN architecture and design documentation, including network diagrams, device configurations and security.
- E. Evaluate the VA wireless LAN architecture for redundancy, reliability, and performance.
- F. Review the existing VA Cisco Wireless LAN Controller deployment and provide recommendations for improved redundancy and scalability.
- G. Analyze VA wireless device configurations and compare with Cisco recommended best practices and SD wireless baselines.
- H. Identify security vulnerabilities in the VA wireless LAN infrastructure.
- I. Provide a summary of the performance gaps in the VA wireless LAN infrastructure.

- J. Document gaps in architecture, security risk analysis, and performance analysis, providing prioritized recommendations for improvement.
- K. Review the existing VA Wireless Cisco ISE (RADIUS) deployment and provide recommendations for improved redundancy and scalability.
- L. Analyze VA Wireless Cisco ISE (RADIUS) device configurations and compare with Cisco recommended best practices and SD wireless baselines.
- M. Evaluate the VA Wireless Cisco ISE (RADIUS) architecture for redundancy, reliability, and performance.

The Contractor shall deliver the Wireless LAN Architecture Design Review Report utilizing Cisco standard practices covering Cisco Wireless LAN Network Infrastructure architecture assessments and elements. The use of web tools, dashboards, and other online applications in support of this requirement is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. Wireless LAN Architecture Design Review Report

5.5.15.2 STABILITY AUDIT

The Contractor shall provide one stability audit per PoP for the following items for Cisco Wireless LAN Network Infrastructure:

- A. Network Improvement Plan
- B. Hardware Field Notice Report
- C. Technology Audit
- D. Hardware Service report
- E. Hardware End of Life/Support report
- F. Custom configuration report
- G. Configuration Best Practices report
- H. Software infrastructure and security report
- I. System log analysis report

The Contractor shall deliver the Wireless LAN Stability Audit Report utilizing Cisco standard practices covering network performance assessments. The use of web tools, dashboards, and other online applications in support of this requirement is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. Wireless LAN Stability Audit Report

5.5.16 BUSINESS CISCO WIRELESS LAN NETWORK CONSULTING

The Contractor shall provide four Business Cisco Wireless LAN Network Infrastructure Strategy Roadmap reports per PoP for the following items for the Cisco Wireless LAN Network Infrastructure:

- A. Analysis of current and planned projects
- B. Development of ROI models
- C. Use case analysis and mapping to projects

The Contractor shall deliver a Wireless LAN Network Infrastructure Strategy Roadmap Report utilizing Cisco standard practices covering Wireless LAN Network Infrastructure deployments. The use of web tools, dashboards, and other online applications in support of this report is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. Wireless LAN Network Infrastructure Strategy Roadmap Report

5.5.17 TELEPRESENCE (BUSINESS VIDEO) OPTIMIZATION SERVICE

The Contractor shall provide Cisco TelePresence (Business Video) Optimization Service in support of the VA EVTN. Contractor support shall consist of the following individual service elements:

5.5.17.1 ARCHITECTURE/STABILITY REVIEW-EVTN

The Contractor shall provide one annual EVTN Architecture/Stability Review per PoP covering the following topics in support of EVTN:

- A. Aggregate System Scalability (Unified Call Manager, Video Communication Servers 9 (VCS) (Control and Expressway, Multipoint Control Units (MCU) Content Recorders, and Management Systems).
- B. Interoperability of all key infrastructure devices.
- C. Overall Desktop client and Hardware Codec configurations.
- D. Overall security posture of key systems and applications
- E. Configuration Best Practices report
- F. System log analysis report
- G. Additional elements

The Contractor shall deliver the Architecture/Stability Report utilizing Cisco standard practices covering network performance assessments. The use of web tools, dashboards, and other online applications in support of this requirement is required. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. EVTN Architecture/Stability Review Report

5.5.18 BUSINESS VIDEO STRATEGY CONSULTING

The Contractor shall provide one EVTN Business Video Strategy Roadmap report per PoP for the following items for EVTN:

- A. Analysis of current and planned projects
- B. Development of ROI models
- C. Use case analysis and mapping to projects

The Contractor shall deliver a Business Video Strategy Roadmap Report utilizing Cisco standard practices covering business video deployments. The use of web tools, dashboards, and other online applications in support of this report is required.

The Contractor shall deliver up to two Business Video Strategy Consulting sessions annually not to exceed four hours in length per session on a topic requested by the TPM to include remote lab access. This report shall be due within 60 days of the topic/location being provided by VA.

Deliverable:

- A. EVTN Business Video Strategy Roadmap Report

5.5.19 CISCO FOCUSED TECHNICAL SUPPORT SERVICES

The Contractor shall provide Cisco's HTOM coverage for all covered products with Cisco's back up and escalation support. Cisco's HTOM shall provide case management services, trending analysis, and escalation tracking/verification. The HTOM shall also directly support the NCE teams as necessary. The Contractor shall also support Asset and Cisco Portal Management to include Inventory Collection Tools and limited Cisco Digital Network Architecture (DNA) appliance support.

5.5.19.1 HIGH TOUCH OPERATIONS MANAGER

The Contractor shall provide at a minimum one Cisco HTOM whom shall support VA operations remotely. The HTOM shall champion VA technical support needs and requirements, correlate VA open cases, and align the correct resources to resolve cases. The HTOM shall reduce the amount of time engineers spend on the phone describing problems, networks, and operations. In addition, the HTOM shall follow-up on all cases. The Cisco HTOM shall limit the impact of the geographical dispersion of VA network infrastructure, by ensuring different troubleshooting groups are not independently spending support hours attempting to resolve the same support issue without coordination. HTOMS shall be listed on the Contractor Staff Support Roster.

5.5.19.2 CASE MANAGEMENT

The Contractor shall deliver Cisco HTOM support providing operations and case management access, for all sites and covered devices/applications, to operations management and case management staff to include the following:

- A. Daily prioritization and support of open Cisco support cases; monitoring of all Product Returns and Replacements (RMA) and entitlement issues. This will include any issues with systems identified as mission critical and not available in the required timeframe.
- B. Daily coordination of Cisco support organizations and VA resources for Cisco support cases.
- C. Provide a single point of contact for operations and process issues. If the HTOM is on leave, a back-up HTOM shall be provided.
- D. The HTOM shall provide an element of the Monthly Status Report, which details the number and type of support cases opened and provide a listing of any open support cases at the time of report. This reporting can be combined with the Monthly Steering reports.
- E. The HTOM shall track the daily progress of open support cases and expedite outstanding issues to ensure the shortest Mean Time to Repair (MTTR) as well as devices designated as mission critical.
- F. Data shall be analyzed, at least monthly, to determine if any critical issues highlight operational abnormalities and gaps. The analysis shall be documented and delivered in the Monthly Status Report. When abnormalities or gaps are identified they shall be brought to the attention of the COR, PPM, or appropriate Technology Program Manager immediately and reported to management on the next business call. Analysis shall include:

1. Monthly review and report of cases and operations activities
2. Project Status
3. RMA Identification
4. Technology Focus
5. Analysis of Critical issues – Stage (S)1/S2
6. Postmortems
7. Analysis of escalation processes
8. Cases categorized by product type, case priority, and Cisco software release
9. Executive summary and recommendations.
10. As required for new staff or staff taking on new job roles, instructional sessions shall be provided on how to best utilize Cisco support web tools and other Cisco troubleshooting tools. At least annually, a Webinar for all VA staff shall be provided which highlights the tools and resources available for use. Summary highlights of the Webinar shall be included in the Monthly Status Report.
11. Upon request, the HTOM may also proactively open a Cisco TAC case to support scheduling of on-call resources in preparation for a planned scheduled change that VA identifies may be of high risk. The Contractor and HTOM shall review the planned change and have resources available, on an on-call expedited basis, in the event that difficulties occur during implementation of the planned change.

5.5.19.3 ASSET AND CISCO PORTAL MANAGEMENT SUPPORT

The Contractor shall provide Asset and Cisco Portal Management Support for VA operations. This support will include all Premium Asset Management Services as defined at

https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/asset-management.pdf

In the event Cisco changes its Premium Asset Management Services during the period of performance of this contract, the Contractor agrees it will not provide services at a reduced level to what is currently maintained at the time of contract award.

In addition, the Contractor shall support VA oversight and administration of these critical Cisco hosted asset portals:

- A. Smart Net Total Care Portal (also known as Cisco Services Connection)
- B. Cisco Software Central (to include all license management capabilities-Traditional, SMART, and Enterprise Agreements)

Support will include user training, user support, and general administrative portal management support. These services and engagements will be managed by the COR and PMs. Reporting on this support will consolidated with the monthly status report as defined in this PWS. Reporting will cover opened/closed support requests, training requests, and general administrative support requests during the reporting period.

5.5.19.4 INVENTORY COLLECTION TOOLS

The Contractor shall provide, maintain, and support Cisco's management and support application known as CSPC as defined under the Cisco Asset Management Service. The Contractor will host this application on VA provided hosting platforms and shall coordinate all updates on this application with the COR and PM. This support shall continue during the full PoP. VA's TMS

shall be used to provide additional data elements necessary for support of VA's installed base of TelePresence systems.

The Contractor shall use CSPC and TMS to provide and support inventory reports under this PWS to VA on an ad hoc basis, but no less than quarterly, including hardware installed, model and serial number information, configuration details, software version and when the device/component goes end of support. These reports assist VA in its hardware refresh planning efforts. Reports shall also be available via a dedicated and secure Cisco SmartNet portal with VA defined access.

CSPC and TMS systems shall also be utilized to improve security advisory analysis to indicate to VA how vulnerable we are to any Cisco issued PSIRT. CSPC shall also be utilized for best practice reporting to include; monitoring software conformance to VA published system standards and baselines and VA goals, with respect to minimizing the number of installed software versions in use by VA for any specific model of Cisco gear in our enterprise.

Combined CSPC /TMS Derived Improvement Reports shall be provided and delivered, by the Contractor from Cisco Project Manager's, within three business days of request by VA, but no less than quarterly.

Deliverable:

- A. CSPC/TMS Derived Improvement Report

5.5.19.5 CISCO DIGITAL NETWORK ARCHITECTURE (DNA) CENTER DASHBOARD AND APPLIANCE LIMITED SUPPORT

The Contractor shall provide, maintain, and support a limited set of Cisco's management and support applications known as Cisco DNA Appliance(s) up to a maximum of 20 instances and the associated DNA Center Dashboard. The Contractor will provide program support to include; technical, configuration, reporting, operational requirements and shall coordinate all updates on these appliances with the COR and designated DNA PM Manager. This will include all required testing elements as defined by VA. This support shall continue during the full PoP or until VA determines a final status of DNA use in the VA environment.

There will be an annual report on the inventory of all Cisco provided DNA Appliance Devices to include serial number, hostname, IP address, and location. This hardware inventory will be added to the IB inventory value as noted in paragraph 5.5.25 of this PWS. The initial report of these appliances shall be delivered in 30 business days of award.

Deliverable:

- A. Cisco DNA Appliance Report

5.5.20 KNOWLEDGE TRANSFER, MENTORING, AND TRAINING SUPPORT

5.5.20.1 GENERAL KNOWLEDGE TRANSFERS

The Contractor shall provide Cisco virtual knowledge transfer and mentoring for the approximately 375 IT infrastructure support employees nationwide that provide Campus LAN management, Wide Area Network Management, UC Support, IP Telephony Support, Data Center/Unified Computing support, and TelePresence support. Quarterly/Monthly knowledge transfer and mentoring presentations shall be provided as needed to include informal technical

update training on a topic that is mutually agreed upon between the Contractor, COR, PPM, TPM, SD and IO Service Line Management. Training shall be delivered virtually by methods to include data sharing (WebEx, Lync), and audio. These training sessions shall be recorded and made available for future use by VA OIT staff.

In addition, on an ad hoc basis (estimated at 10 per quarter), the Contractor shall provide and deliver white papers, design guides, case studies, configuration guides, troubleshooting guides, deployment guides, and training documents on Cisco technologies relevant to discussions with VA where the papers and guides would help enhance VA's understanding of Cisco products and their capabilities. In addition, whenever requested by VA, the Contractor shall provide informal ad-hoc training as required (estimated at one per quarter), on a specific agreed upon topic.

The Contractor shall deliver Cisco Business Critical Services staff provided collateral training materials utilized in localized training or knowledge transfer sessions with VA staff to the VA COR, PPM, and TPM for internal posting and viewing by VA personnel, within 72 hours of creation and approval of the material.

Deliverables:

- A. Monthly Knowledge Transfer Sessions
- B. White Papers
- C. Design Guides
- D. Case Studies
- E. Support and Configuration Guides
- F. Troubleshooting Guides
- G. Deployment Guides
- H. Training Documents

5.5.20.2 CISCO LEARNING CREDITS

To support deep understanding of deployment, configuration, and maintenance of Cisco technologies by VA staff, Cisco Learning Credits (CLC) shall be provided which allows VA IT support staff to attend classroom based or virtually hosted Cisco courses. The Contractor shall deliver the following CLC features:

- A. All CLCs provided shall be valid for at least one year upon activation.
- B. An online tool shall be provided allowing VA to manage and track 24x7, CLCs owned, assigned and redeemed for each user.
- C. CLCs provided shall be redeemable through authorized Cisco Learning Solution Partners and their affiliated organizations or Cisco Virtual Live Online training.
- D. A single CLC shall be worth \$100 US dollars of training.

The Contractor shall deliver an initial firm quantity of 5,125 CLCs each base and option period to ensure that each of the approximately 375 OIT Employees can attend one class each per base and option year, for a course that costs, on average, 35 credits to attend. The Government may authorize additional CLCs over and above the 5,125 CLCs provided with the base and options periods on an as-needed basis not to exceed 4 lots of 2,000 CLCs for a total of up to 13,125 CLCs in a single PoP. At the conclusion of the base and each option period, the remaining balance of CLCs that are not authorized for use will be de-obligated from the PoP. The initial quantities of CLCs per PoP shall be delivered within 30 business days of award. All lot requests of CLCs in a PoP shall be delivered within 15 business days of a VA request and invoiced.

All CLCs shall be delivered to a VA designed Learning Credit Management Tool (LCMT) account. The VA will designate a team captain to manage this account. All future VA procurements of Cisco systems from all contract sources that include additional CLCs shall be captured and deposited in this same account.

Deliverables:

- A. Cisco Learning Credits, quantities as defined per PoP

5.5.20.3 TECHNICAL KNOWLEDGE LIBRARY (TKL)

The Contractor shall provide specified VA IT staff with 24x7x365 direct access to Cisco's TKL. The number of staff who may receive direct access to TKL is unlimited. The TKL shall be made available via a secure web-based portal ("Portal"). Cisco's Network Knowledge Service shall provide on demand access to Cisco's knowledge resources including:

- A. Intellectual property such as leading practices documentation, whitepapers, case studies, and configuration examples.
- B. Knowledge transfer sessions captured as video on demand.
- C. Self-study and e-learning resources including Networkers Online, Cisco Press books (in PDF), deployment kits, Cisco Interactive Mentor, e-learning courseware, and live remote labs.
- D. Access exclusive content not available on Cisco.com.
- E. Multimedia clips in the form of video on demand or audio on demand content.
- F. Sidebar content such as white papers, case studies, design guides, configuration guides, troubleshooting guides, training documents, deployment guides, online textbooks and/or manuals, or bumper clips.
- G. Listed web-based trainings provided via the TKL to authorized viewers.
- H. Preventative maintenance in accordance with Cisco's normal maintenance schedules and procedures.
- I. Troubleshooting assistance for issues submitted to Cisco.
- J. Updated content as Cisco may revise, update, and/or remove previously-released multimedia clips and/or sidebar content ("updated content") and whereby Customer should discontinue any use of superseded content.

The list of VA staff needing access to the TKL will be provided via the COR and PPM, through the VA designed Education TPM, no less than annually. However, due to changes in staffing and job responsibilities, VA reserves the right to add or remove staff with access to the TKL. TKL Portal entitlement for all VA users begin within seven business days of award.

5.5.20.4 CISCO PLATINUM LEARNING LIBRARY (CPLL) ACCESS

The Contractor shall provide 200 perpetual eLearning Training All Technology Groups licenses for VA use throughout the base and all option periods of this agreement. This will allow assignment of access to VA staff to support on-line training in the five technology libraries to include Networking, Security, Data Center, Collaboration, and Cloud. The COR/PPM shall designate VA staff to support and manage this program as an Education TPM. Usage of these licenses will be tracked and reported during the Monthly Status Report and any general business meeting. Format of this reporting will be determined by the VA designed Education TPM with coordination via the COR and PPM. Access to these CPPL Licenses shall be provided within 30 business days of award.

Deliverables:

A. CPLL Licenses

5.5.20.5 CISCO MODELING LABS (CML) CORPORATE EDITION PLATFORM

The Contractor shall provide annual term subscription support for all VA utilized CML licenses during the base and all option periods as follows:

Description/Part Number	Quantity
CML CE SW v1.x subscription with 15 nodes/R-CML-CE-K9=	2
Cisco Modeling Lab (CML) 1-year base license (required) includes 15 Nodes/CML-CE-1Y	2
CML CE 50 nodes expansion/L-CML-CE-50N=	2
CML CE 50 nodes expansion 1Yr/CML-CE-50N-1Y	2
CML CE 100 nodes expansion/L-CML-CE-100N=	2
CML CE 100 nodes expansion 1Yr/CML-CE-100N-1Y	2

Support will include TAC access and technical support as required. These shall be reported and included in the IB in the same manner as CSR 1000V. These shall be delivered annually as necessary to ensure that no node license expires.

Deliverables:

A. Annual CML Licenses

5.5.21 CBCESA INVENTORY MANAGEMENT**5.5.21.1 MASTER INVENTORY REPORTING**

The Contractor shall be responsible for all inventory reporting and reconciliation/true-up and true forward requirements as defined under this section of the PWS. There will be two elements that constitute the overall Inventory management process. The Contractor may provide either separate reports for each set of requirements or a single integrated report which contains all the same report elements as defined below. Use of on-line reporting portals with VA access and notifications is encouraged. The Contractor shall coordinate all Inventory reporting work with any Contractor assigned Asset and Cisco Portal Management Support personnel. The VA COR and PPM shall review and approve the final reporting format for all inventory reporting elements. Once approved no changes will be made to the approved reporting format unless directed by the VA COR/PPM.

5.5.21.2 INSTALL BASE REPORT

The Contractor shall conduct quarterly inventory reconciliations as defined in paragraph 5.5.21.5 to monitor and manage the IB inventory database. The Contractor shall provide and deliver quarterly an updated IB Inventory Database Report for VA concurrence. The IB Inventory Report shall be in a spreadsheet, database or other VA approved format to include at a minimum the following: item nomenclature, part number, serial number, location (if available), list price, support expiration date, equipment category, and equipment SNTC Service Levels, products marked for mission critical services, and shall highlight changes from the prior quarter's IB inventory. Maintenance of support applications, list price and associated device license keys shall be documented using the same method. For advanced planning purposes, the report shall contain an inventory of items whose SNTC service was previously purchased and still is in

effect, but is not included in the IB. This shall include its current SNTC expiration date for future inclusion in the IB at the time of expiration of current coverage. Use of the elements in the IB provided in Attachment 1 is recommended.

The IB shall incorporate the VA Managed Cisco CSR 1000V Routers after the initial listing is provided as Attachment 2 to include the following: item nomenclature, part number, serial number (UUID), PAK number, location, support expiration date to include licenses and terms, and equipment Smart Net Service Levels, and shall highlight changes from the prior year's inventory. The IB shall also include the Cisco DNA Appliances and CML license value and the Cisco CUSP and CUBE as described in paragraphs 5.3, 5.5.19.5 and 5.5.20.5.

Deliverable(s):

A. IB Inventory Database Report

5.5.21.3 CISCO COLLABORATION FLEX SERVICE REPORT

The Cisco Collaboration Flex Service Report shall track and report the following on a quarterly basis to monitor and manage the Cisco Collaboration Flex service inventory:

Total Active Knowledge Workers
Total PBX Calling Users
Total Contact Center Concurrent Agents
Total Active Meeting Hosts/Users

This report shall be used for True Forward reconciliation as defined below.

Deliverable(s):

B. Cisco Collaboration Flex Service Report

5.5.21.4 CBCESA INVENTORY RECONCILIATION/TRUE-UP AND TRUE-FORWARD

VA's Cisco product and system inventory, during any PoP, shall be permitted to fluctuate upward or downward during the applicable PoP without any price adjustment. There will be two parallel but distinctive processes for Inventory Reconciliation/True-Up and True-Forward. These two processes will also determine the total base value of covered products and services for this requirement. This will be reported as a standard IB Inventory Database and Cisco Collaboration Flex Service Report.

5.5.21.5 INSTALL BASE RECONCILIATION/TRUE-UP PROCESS

This process shall apply only to the IB which shall include the Cisco CSR 1000V Routers, CML inventory, and CUSP and CUBE inventory. The Contractor shall provide Cisco SNTC and SWSS for all systems as defined in PWS paragraph 5.2 and for all Cisco inventory added to the IB during the PoP.

The Contractor shall perform a final inventory reconciliation/true-up and value annually, conducted within 60 days prior to the end of the PoP for that period. The Reconciliation/True-up shall allow for the following:

1. Additions of inventory caused by the procurement of software licenses and hardware since the last IB was established to include Cisco CSR 1000V Routers.

2. Subtractions of inventory caused by the expiration of licenses/units, reductions in software products and/or removal of Cisco hardware products owned within the VA Enterprise since the last true-up. If equipment is to be retired, VA will notify the Contractor.
3. Cisco software or hardware inventory purchased and in use by VA, which does not have valid SNTC service, shall be included in the IB calculation for support. In use is defined as Cisco gear reporting to the CSPC or the Enterprise Video Teleconferencing Network (EVTN) TMS, or which has been purchased and is in use by VA but is incapable of reporting to the CSPC or TMS, or equipment which has been purchased by VA but remains in a Ready Spare status. The Contractor may coordinate collection of all VA awarded contracts that contain Cisco systems and applications with the assigned asset manager for inclusion in the IB to facilitate capture of these at the earliest opportunity.
4. Cisco software or hardware inventory going End of Support in the current contract PoP shall be deleted from the IB calculation each year.
5. Cisco software or hardware inventory purchased which includes SNTC Services coverage at time of purchase shall not be included in the IB inventory until after its current SNTC Services coverage expiration date.
6. Cisco software or hardware inventory which has been declared lost due to an event beyond the control of VA as described in 5.5.21.5 shall be removed from the IB inventory.
7. The Cisco CSR 1000V routers, CML, and Cisco CUSP/CUBES will be included in the IB for the purposes of this calculation inclusive of all SWSS and Annual Term Licensing Costs.

These inventory items shall remain in the IB inventory and shall continue to be covered under the SNTC, SWSS services as defined in this PWS. This total IB value will be used to define the price band for the next PoP.

The reconciliation/true-up process shall allow for significant equipment loss due to an event beyond the control of VA including but not limited to any Act of God, terrorism, war, political insurgence, insurrection, riot, civil unrest, act of civil or military authority, uprising, earthquake, flood, fire or any other natural or manmade disaster outside of VA's control. VA will provide an equipment list that has been damaged or lost and the Contractor shall subtract the lost equipment inventory from the IB within 30 days of VA notification. If the reduction of the installed base inventory due to an event beyond the control of VA causes a change in price band, the Contractor shall apply a cost credit on the unused services to the current PoP, which shall result in a de-obligation of funds to reflect a lower price in the IB Band.

The Contractor shall track and tag but not include any VA inventory into the IB whose SNTC was procured at the time it was initially procured and the SNTC Service is still valid. The Contractor shall add these items to the IB when the current SNTC Service has expired, or as determined by the COR and PPM for immediate inclusion to ensure continuous support.

Reconciliations/true-ups shall continue through each exercised option period within 60 days of the end of the base year and each following 12-month option period. The annual Reconciliation/true-up will establish the IB inventory for the next PoP. The Contractor shall reconcile and document any/all inventory changes with VA concurrence in each option year

The result of this reconciliation/true-up process will determine the IB inventory and value for the next PoP. Any additional inventory added during this 60-day period will be included in the next IB Inventory Database Report.

5.5.21.6 CISCO COLLABORATION FLEX SERVICE INVENTORY TRUE-FORWARD PROCESS

This process shall apply only to the Cisco Collaboration Flex Services. Adjustments or True-Forwards of this service inventory shall occur within 90 days prior to the end of each PoP.

The Contractor shall access the VA Cisco Enterprise Agreement (EA) Workspace and determine the number of Knowledge Workers who have used computing or communications devices capable of running the Contractor provided Cloud Services and using the software as defined in this PWS as part of their job duties. Knowledge Worker count also includes the employees of any VA affiliate that may use these services.

Utilizing the Cisco provided cloud hosted services the Contractor shall meter and determine the Total Active Meeting Hosts that have initiated at least one “Meeting” in Webex Meetings, Webex Teams, or by phone using a Webex personal conferencing number. This measurement shall be averaged out in months 9, 10, and 11 of each PoP. This average shall be used as the base for the next PoP.

Upon written request from the Contractor, VA will assist and make information available to facilitate verification of the number of Concurrent Agent Contact Center services or software licenses that have been installed, accessed, deployed, or activated. VA and Contractor shall agree that this Concurrent Agent Contact Center count is a true and valid count for the purposes of true-forward.

The result of this true-forward process will establish the number of Concurrent Agent Contact Center services or software licenses that have been installed, accessed, deployed, or activated for purposes of establishing the service inventory for the next PoP. Any additional licenses installed, accessed, deployed, or activated during this 90-day period will be included in the next true-forward.

The annual CBCESA price of this service for the next PoP shall be adjusted to reflect the service inventory as a result of the true-forward process.

The total value of all Cisco Collaboration Flex Services for the Base Period shall be based solely on the initial counts as defined in paragraph 5.4.3 of this PWS.

The price for Cisco Collaboration Flex Services in the Option periods shall be based on the Cisco Collaboration Flex True-Forward Inventory as determined by the true-forward process set forth herein.

5.5.22 CBCESA USER ACCESS AND REPORTING

The Contractor shall forward electronically all requests from all sources for the addition of authorized users to this agreement to the COR and PPM for review and approval prior to authorization. Access may not be granted without VA approval. The Contractor shall provide on a semi-annual basis a CBCESA User Access report of all users authorized to use this agreement for review and updates. The COR and PPM shall review and provide any required updates and

changes, and actions to the Contractor. The Contractor then shall complete all required changes within five business days. This will include users with access to the CNS as defined in PWS paragraph 5.3.1. Access to other Cisco current or future “portals” will be managed and approved via Cisco defined processes.

Deliverable:

A. CBCESA User Access Report

5.6 SYSTEM AND ORGANIZATIONAL CONTROLS (SOC) FOR SERVICE ORGANIZATIONS REPORTING REQUIREMENTS

5.6.1 SERVICE ORGANIZATION CONTROL (SOC) REPORTING

The Contractor shall engage an independent external auditing firm to conduct a Service Organization Controls (now called System and Organizational Controls (SOC) for Service Organizations) examination and produce a Report on Controls at a Service Organization Relevant to Security of VA provided data use of Cisco hosted Webex and Webex Teams systems Contractor hosted Information and Systems, Processing Integrity, Confidentiality, and Privacy, SOC 2 Type 2 Report, (the “Prime Report”) in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No. 18, Attestation Standards: Clarification and Recodification (SSAE 18). The Contractor shall provide VA with a written copy of the SOC 2 Type 2 examination report (the “Prime Report”). In addition, the Contractor shall provide a written copy of the SOC 2 Type 2 report, completed in accordance with SSAE 18, for any material subservice organization (the “Subcontractor Report”). The Prime Report and Subcontractor Reports must address the specific services provided by the Contractor to VA under this contract. The current guidance for SSAE 18 was issued in April 2016. Reference:

https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf (Section 320, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities’ Internal Control Over Financial Reporting). SSAE guidance may be updated during the performance of the contract. The Contractor shall comply with updates to SSAE 18 and provide new reports using the updated SSAE guidance.

The report shall cover all trust principles to include: Security (of Information and Systems), Availability (of Information and Systems), Processing Integrity, Confidentiality, and Privacy and ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA) under those principles.

5.6.2 SERVICE ORGANIZATION CONTROL REPORTING - SPECIFICATIONS AND DELIVERABLES

VA’s fiscal year begins October 1 and ends on September 30. The Contractor shall submit an initial Prime Report and Subcontractor Reports – SOC 2 for all current business and financial operations, or address specific services to include use of Cisco hosted Webex and Webex Teams systems provided by the Contractor to VA under this contract. The initial report shall cover a minimum of nine months of contract performance in accordance with the Schedule of Deliverables. Any deviation to the initial report minimum period must be approved by VA.

Subsequent Prime Reports and Subcontractor Reports shall cover twelve-month periods and be submitted in accordance with the Schedule of Deliverables. Such subsequent reports shall cover the specific services provided by the Contractor to VA under this contract.

All Prime Reports and Subcontractor Reports shall clearly indicate the services, systems, and locations covered by the review, as well as the nature and type of control testing performed. The Contractor shall also account for controls over subservice organization (Subcontractor) services and performance. The Contractor shall include a cover letter on all Prime Reports and Subcontractor Reports affirming that the Contractor is performing services in accordance with the contract. The cover letter shall be addressed to VA and summarize the results of the audit and the audit tests performed. The letter shall highlight unusual items, deficiencies, qualifications, and any inconsistencies with professional standards and provide an indication of actions being taken to address, remedy, or mitigate these or other weaknesses noted in the applicable report.

In the event a Prime Report or Subcontractor Report includes any deficiencies material to the Contractor's performance under this contract or significant to VA's internal controls over financial reporting or operational controls to achieve the VA mission, as determined by VA in its sole discretion, VA will notify the Contractor in writing of the need for a Corrective Action Plan (CAP) within 30 days of receipt of the Prime Report. The Contractor shall submit the CAP to VA in accordance with the Schedule of Deliverables. The CAP shall describe, in detail, actions that will be taken by the Contractor to resolve the deficiencies and the timeline (begin and end dates) for completing each action. The Contractor shall implement recommendations from its auditor and the audit report within 90 days from report issuance and must cure any deficiencies to VA's satisfaction within a reasonable period, but no later than 90 days from report issuance, and at no additional cost to VA.

The Contractor shall provide a Bridge Letter in accordance with the Schedule of Deliverables to cover the dates between the applicable Prime Report's and Subcontractor's Report period end date and VA's fiscal year end date (September 30) or the end date of all performance under the contract.

The Contractor shall address the Bridge Letter to VA from Contractor senior management and must specify the coverage begin and end dates. The letter shall include Contractor management's assertion whether the processes and internal controls that were in effect during the period covered by the applicable Prime Report and Subcontractor Reports remain in effect, and/or summarize any material changes in the control environment and the impact to VA. The Bridge Letter is not a replacement for the actual Prime Report or Subcontractor Reports.

The VA COR, PPM, and Information Systems Security Officers (ISSO) will oversee and manage this requirement.

Deliverable:

A. CBCESA Prime Report and Subcontractor Reports – SOC 2
CBCESA SOC Bridge Letter (as required)

5.7 RIGHTS IN COMMERCIAL LICENSES AND TECHNICAL DATA AND REPORTS

The Contractor is required to deliver technical data, configurations, documentation or other information during contract performance specifically the following written deliverables Deployment Guides (CLINs X005BN), Troubleshooting guides (CLINs X005BM) and training documents (CLINs X005BP) and any other written deliverables first produced and delivered during contract performance. 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 any and all documentation created in support thereof. License rights in any Commercial Computer Software inclusive of Cisco Platinum Learning Library Licenses and Annual Cisco Modeling Labs Licenses shall be governed by FAR 52.227-19, Commercial Computer Software License (DEC 2007).

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with VA TRM. The 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. Moreover, the VA TRM, which includes the Standards Profile and Product List, serves as a technology roadmap and tool for supporting OIT. Architecture & Engineering Services (AES) has overall responsibility for the VA TRM.

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

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

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

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at:

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf>,

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf>, and

<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>

respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

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

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

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

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005

(<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010

(https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-

[ipv6.pdf](#)). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-267.pdf>), the Technical Infrastructure for USGv6 Adoption (<https://www.nist.gov/programs-projects/usgv6-program>), and the NIST SP 800 series applicable compliance (<https://csrc.nist.gov/publications/sp>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2.2_2017.pdf.

6.1.5 STANDARD COMPUTER CONFIGURATION

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

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient

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

6.1.7 PROCESS ASSETT LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL). The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf. The main PAL can be accessed at www.va.gov/process.

6.1.8 AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall Enterprise Architecture (EA) that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department's Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below. The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor and vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with Vet360 to access personal contact information, if the solution relies on VA Veteran personal contact information data. Vet360 is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying

active duty military service data. VADIR is the authoritative source for Qualifying Active Duty military service in the VA.

6.2 SECURITY AND PRIVACY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

	Position Sensitivity and Background Investigation Requirements		
<u>Task Number</u>	<u>Low/NACI</u>	<u>Moderate/MBI</u>	<u>High/BI</u>
5.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
5.6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

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 specific 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. These security requirements do not apply to TAC support personnel and apply only to assigned Contractor Support Staff, HTOMs, and NCEs that require VA network access to perform the requirements under this PWS.

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. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster as defined in paragraph 5.1.2 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.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
 - d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) Optional Form 306
 - 2) Self-Certification of Continuous Service
 - 3) VA Form 0710
 - 4) Completed SIC Fingerprint Request Form
 - e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the 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).
 - f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
 - g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
 - h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
 - i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
 - j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
 - k. 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.

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 2010/2016, MS Excel 2010/2016, MS PowerPoint 2010/2016, MS Project /2010/2016, MS Access 2010/2016, MS Visio 2010/2016, AutoCAD 2015-2019, 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(s)	Acceptable Performance Levels
A. Meeting Technical Needs	<ol style="list-style-type: none"> 1. Demonstrates understanding of technical and support requirements 2. Efficient and effective in meeting overall technical requirements 3. Provide access to technical assistance center 24x7x365 4. Provide access to knowledge base, tools software updates, developers, and business units 5. Manages Install Base and Inventory Reconciliation 6. Provide Business Critical & Optimization Services 7. Provide Hosted Lab Cycles 8. Supports Cisco Commo8 Services Platform Collector (CSPC) in VA 	Satisfactory or higher
B. Project Milestones and Schedules	<ol style="list-style-type: none"> 1. Meets established milestones and project dates 2. Products, reports, invoices, and deliverables are reviewed and delivered in a timely manner 	Satisfactory or higher

Performance Objective	Performance Standard(s)	Acceptable Performance Levels
	3. Notifies customer in advance of problems meeting milestones and schedules	
C. Program Staffing	1. Currency of contractor expertise 2. Personnel possess the necessary skills and ability to accomplish tasks 3. Staffing levels are appropriate PWS requirements	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The Government 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 manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.4.1 DELIVERABLE METRICS/SERVICE LEVEL AGREEMENTS (SLA)

This section contains the tables and descriptions that provide VA SLA framework and expectations relating to service level commitments. This section defines VA detailed performance, management, and reporting requirements for the CBCESA. All service level requirements as defined in the table below constitute the overall SLAs for this service. TAC Case Response, TAC Case Restoration of Service, and Mission Critical times shall be reported monthly. This calculation will be used to determine the level of SLA performance and the percentage value of the FFP that shall be paid by VA for the next monthly invoice if the performance is below the stated SLA requirement. The Government will conduct a monthly review of the defined SLAs against the Contractors provided data and the CBCESA SLA Monitoring Plan. All SLA metrics shall be rounded up to the closest whole number. No fractional metrics for the final measurement period shall be used.

The Contractor shall meet the required SLA as described in the PWS. However, if the Contractor's performance falls below a required service level identified in the table below, the Contractor shall only be paid for the lower service level provided. Please be advised that the VA's payment for the lower service level provided in no way waives the Government's right to pursue any remedies available by law, including, but not limited to, termination for breach of contract.

The Contractor's failure to meet the Deliverable Metrics/Service Level Agreements as set forth in this PWS shall be considered a condition endangering contract performance and may provide grounds for default termination. The Contractor will not be faulted for lower service levels that occur due to external circumstances beyond the Contractor's control. Any conditions that the Contractor considers relevant to this calculation shall be included in the CBCESA SLA Report.

For any PWS task in which there are multiple SLAs, the credit will be calculated for the lowest service level provided. Furthermore, each metric stands alone, therefore, if a single event impacts multiple SLAs across PWS Tasks, the Contractor shall be paid for lower service provided for all of the tasks that were impacted.

SLAs are set forth in PWS Firm-Fixed-Price tasks 5.2.1 and 5.2.3.1. The following table provides the calculation and measurement of each Firm-Fixed-Price (FFP) Deliverable Metric/SLA specified. Measurement of Deliverable Metrics/SLAs shall begin 30 days after Government acceptance of the CBCESA SLA Monitoring Plan.

SLA ID	PWS Task	SLA	SLA Metric	Percentage of base FFP monthly payment to be paid by VA
1	5.2.1	TAC Case Response: Severity 1 (S1) and 2 (S2)	No less than 95% of S1 and S2 cases meet the SLA response times during the measurement period.	0% reduction of FFP
			94% to 92% of S1 and S2 cases meet the SLA response time during the measurement period.	.1% reduction of FFP
			91% to 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.2% reduction of FFP
			Below 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.5% reduction of FFP
2	5.2.1	TAC Case Response: Severity 3 and 4	No less than 95% of S1 and S2 cases meet the SLA response times during the measurement period.	0% reduction of FFP
			94% to 92% of S1 and S2 cases meet the SLA response time during the measurement period.	.1% reduction of FFP
			91% to 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.2% reduction of FFP
			Below 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.5% reduction of FFP
3	5.2.1	TAC Case Restoration of Service: Severity 1 and 2	No less than 95% of S1 and S2 cases meet the SLA response times during the measurement period.	0% reduction of FFP
			94% to 92% of S1 and S2 cases meet the SLA response time during the measurement period.	.1% reduction of FFP

			91% to 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.2% reduction of FFP
			Below 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.5% reduction of FFP
4	5.2.1	TAC Case Restoration of Service Response: Severity 3	No less than 95% of S1 and S2 cases meet the SLA response times during the measurement period.	0% reduction of FFP
			94% to 92% of S1 and S2 cases meet the SLA response time during the measurement period.	.1% reduction of FFP
			91% to 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.2% reduction of FFP
			Below 90% of S1 and S2 cases meet the SLA response time during the measurement period.	.5% reduction of FFP
5	5.2.3.1	Mission Critical Delivery	No less than 95% of mission critical deliveries meet the SLA response times during the measurement period.	0% reduction of FFP
			94% to 92% of mission critical deliveries meet the SLA response time during the measurement period.	.1% reduction of FFP
			91% to 90% mission critical deliveries meet the SLA response time during the measurement period.	.2% reduction of FFP
			Below 90% of mission critical deliveries meet the SLA response time during the measurement period.	.5% reduction of FFP

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 Systems Security Officer (ISSO) and Privacy Officer (PO).

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

6.6 GOVERNMENT FURNISHED PROPERTY

The Government has multiple remote access solutions available to include Citrix Access Gateway (CAG), Site-to-Site Virtual Private Network (VPN), and RESCUE VPN.

The Government's issuance of Government Furnished Equipment (GFE) is limited to Contractor personnel requiring direct access to the network to: development environments; install, configure and run VA TRM approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner); upload/download/ manipulate code, run scripts, and apply patches; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

When necessary, the Government will furnish desktops or laptops, for use by the Contractor to access VA networks, systems, or applications to meet the requirements of this PWS. The

overarching goal is to determine the most cost-effective approach to providing needed access to the VA environment coupled with the need to ensure proper Change Management principles are followed. Contractor personnel shall adhere to all VA system access requirements for on-site and remote users in accordance with VA standards, local security regulations, policies and rules of behavior. GFE shall be approved by the COR and Program Manager on a case-by-case basis prior to issuance.

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

1. 20 advanced 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 Personal Identity Verification card readers, peripheral devices, or additional Random-Access Memory (RAM). The Contractor is responsible for providing these types of IT accessories in support of this effort as necessary and any VA installation required for these IT accessories shall be coordinated with the COR.

Additionally, the Contractor shall provide a status of all reportable GFE as part of the Quarterly Status Report as required by PWS paragraph 5.1. For purposes of this report, reportable GFE includes equipment that is furnished by the Government as tangible “personal” property which the Contractor takes possession of, physically leaves a Government facility, and needs to be returned the end of Contractor performance. The following information shall be provided for each piece of GFE:

1. Name of contractor employee assigned to the GFE
2. Type of Equipment (Make and Model)
3. Tracking Number/Serial Number
4. VA Bar Code
5. Location
6. Value
7. Total Value of Equipment
8. Anticipated Transfer Date to Government
9. Anticipated Transfer Location

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System 2.0, and will be tracked therein. The Talent Management System 2.0 may be accessed at <https://www.tms.va.gov/SecureAuth35/>. If you do not have a TMS 2.0 profile, go to <https://www.tms.va.gov/SecureAuth35/> and click on the "Create New User" link on the Talent Management System 2.0 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 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): https://www.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): https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

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

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

A3.1. Section 508 – Information and Communication Technology (ICT) Standards

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule>.

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

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

A3.2. Compatibility with Assistive Technology

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

A3.3. Acceptance and Acceptance Testing

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

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

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 13834, “Efficient Federal Operations”, dated May 17, 2018; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.
4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

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

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

3. Televisions, Multimedia Projectors

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

A7.0 OEM HARDWARE REQUIREMENTS

The Contractor shall ensure that information technology products are procured and/or services are performed with products that are new equipment and new parts for the required services described herein; no used, refurbished, or remanufactured equipment or parts shall be provided under any circumstances. Absolutely no “Gray Market Goods” or “Counterfeit Electronic Parts” shall be provided. Gray market goods are defined as genuine branded goods intentionally or unintentionally sold outside of an authorized sales-territory or by non-authorized dealers in an authorized territory. All equipment shall be accompanied by the original equipment manufacturers (OEM’s) warranty. Counterfeit electronic parts are defined as unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

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 Contractor/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

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

4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

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

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

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

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

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

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

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

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

13. For all data services and privacy requirements that involves the storage, generating, transmitting, or exchanging of VA sensitive information the Contractor or its subcontractor the hosts the actual VA data shall have ISO/IEC 27001 certification from an accredited and respected certification body for their Information Security Management System (ISMS) and shall provide to the VA a copy of the certificate and report annually.

Deliverable:

A. ISO/IEC 27001 Certification

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, but in no event longer than 30 days.

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

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. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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

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

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

6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

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

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

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

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

- 1) Vendor must accept the system without the drive;
- 2) VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
- 3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
- 4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

- a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
- b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
- c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

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-days' notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior, relating to access to VA information and information systems;
 - 2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System 2.0 # VA 10176) and complete this required privacy and information security training annually;
 - 3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
- c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

SECTION C - CONTRACT CLAUSES

C.1 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oal/library/vaar/>

(End of Clause)		
<u>FAR/VAAR</u> <u>Number</u>	<u>Title</u>	<u>Date</u>
52.203-3	GRATUITIES	APR 1984
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER	MAY 2011
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-21	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS	JUN 2016
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS	OCT 2018
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-14	RIGHTS IN DATA-GENERAL	MAY 2014
52.227-16	ADDITIONAL DATA REQUIREMENTS	JUN 1987
52.227-19	COMMERCIAL COMPUTER SOFTWARE LICENSE	DEC 2007
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS	DEC 2013
852.203-70	COMMERCIAL ADVERTISING	May 2018
852.219-9	VA SMALL BUSINESS SUBCONTRACTING PLAN MINIMUM REQUIREMENTS	DEC 2009
852.219-75	SUBCONTRACTING COMMITMENTS MONITORING AND COMPLIANCE (DEVIATION)	JUL 2018
852-232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS	JUN 2013
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.237-70	CONTRACTOR RESPONSIBILITIES	APR 1984
852.270-1	REPRESENTATIVES OF CONTRACTING OFFICERS	JAN 2008

C.2 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS—COMMERCIAL ITEMS (AUG 2019)

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

- (1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
- (3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 89(a)(1)(A) of Pub. L. 115-232).
- (4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)
- (5) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
- (6) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

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

[Contracting Officer check as appropriate.]

- ☒ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).
- ☒ (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).
- ☐ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).
- ☒ (4) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
- ☐ (5) [Reserved]
- ☒ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- ☐ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).
- ☐ (8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).
- ☒ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).
- ☐ (10) [Reserved]
- ☐ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).
- ☐ (ii) Alternate I (Nov 2011) of 52.219-3.

- _X_ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).
- ___ (ii) Alternate I (Jan 2011) of 52.219-4.
- ___ (13) [Reserved]
- ___ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).
- ___ (ii) Alternate I (Nov 2011).
- ___ (iii) Alternate II (Nov 2011).
- ___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
- ___ (ii) Alternate I (Oct 1995) of 52.219-7.
- ___ (iii) Alternate II (Mar 2004) of 52.219-7.
- _X_ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).
- _X_ (17) (i) 52.219-9, Small Business Subcontracting Plan (Aug 2018) (15 U.S.C. 637(d)(4)).
- _X_ (ii) Alternate I (Nov 2016) of 52.219-9.
- ___ (iii) Alternate II (Nov 2016) of 52.219-9.
- ___ (iv) Alternate III (Nov 2016) of 52.219-9.
- ___ (v) Alternate IV (Aug 2018) of 52.219-9.
- ___ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
- ___ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).
- _X_ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- ___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).
- _X_ (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).
- ___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).
- ___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).
- _X_ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- ___ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).
- _X_ (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- _X_ (28) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
- ___ (ii) Alternate I (Feb 1999) of 52.222-26.
- _X_ (29) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
- ___ (ii) Alternate I (July 2014) of 52.222-35.
- _X_ (30) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
- ___ (ii) Alternate I (July 2014) of 52.222-36.
- _X_ (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
- _X_ (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- ___ (33) (i) 52.222-50, Combating Trafficking in Persons (JAN 2019)

- (22 U.S.C. chapter 78 and E.O. 13627).
- ___ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).
- ___ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- ___ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- ___ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).
- ___ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- ___ (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514)
- ___ (ii) Alternate I (Oct 2015) of 52.223-13.
- ___ (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).
- ___ (ii) Alternate I (Jun 2014) of 52.223-14.
- ___ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).
- _X_ (41) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).
- ___ (ii) Alternate I (Jun 2014) of 52.223-16.
- _X_ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).
- ___ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).
- ___ (44) 52.223-21, Foams (Jun 2016) (E.O. 13696).
- ___ (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- ___ (ii) Alternate I (Jan 2017) of 52.224-3.
- ___ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).
- ___ (47) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).
- ___ (ii) Alternate I (May 2014) of 52.225-3.
- ___ (iii) Alternate II (May 2014) of 52.225-3.
- ___ (iv) Alternate III (May 2014) of 52.225-3.
- ___ (48) 52.225-5, Trade Agreements (Aug 2018) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).
- _X_ (49) 52.225-13, Restrictions on Certain Foreign Purchases (June 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- ___ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- ___ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

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

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

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

X (55) 52.232-33, Payment by Electronic Funds Transfer--System for Award Management (Oct 2018) (31 U.S.C. 3332).

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

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

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

X (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).

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

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

___ (iii) Alternate II (Feb 2006) of 52.247-64.

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

[Contracting Officer check as appropriate.]

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

___ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).

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

___ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).

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

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

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

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

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

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

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

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

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

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

(e)

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

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Jan 2019) (41 U.S.C. 3509).

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

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

(iv) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-232).

(v) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

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

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

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

(ix) 52.222-35, Equal Opportunity for Veterans (Oct 2019) (38 U.S.C. 4212).

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

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

- (xii) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
- (xiii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).
- (xiv) (A) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
- (B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).
- (xv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)
- (xvi) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)
- (xvii) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).
- (xviii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).
- (xix) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
- (xx) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
- (B) Alternate I (Jan 2017) of 52.224-3.
- (xxi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (xxii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.
- (xxiii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

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

(End of Clause)

Alternate I (Feb 2000). As prescribed in [12.301](#)(b)(4)(i), delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to “paragraphs (a), (b), (c), or (d) of this clause” in the redesignated paragraph (d) to read “paragraphs (a), (b), and (c) of this clause”.

Alternate II (Aug 2019). As prescribed in 12.301(b)(4)(ii), substitute the following paragraphs (d)(1) and (e)(1) for paragraphs (d)(1) and (e)(1) of the basic clause as follows:

(d)

(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to—

- (i) Examine any of the Contractor’s or any subcontractors’ records that pertain to, and involve transactions relating to, this contract; and
- (ii) Interview any officer or employee regarding such transactions.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), and (c), of this clause, the Contractor is not required to flow down any FAR clause in a subcontract for commercial items, other than—

(i) *Paragraph (d) of this clause.* This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (d)(1)(ii) does not flow down; and

(ii) *Those clauses listed in this paragraph (e)(1).* Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

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

(B) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5).

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

(D) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or

Equipment. (AUG 2019) (Section 889(a)(1)(A) of Pub. L. 115-

232).

(E) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

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

(G) 52.222–26, Equal Opportunity (Sep 2016) (E.O. 11246).

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

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

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

(K) 52.222–41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).

(L) ____ (1) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).

____ (2) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

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

- (N) 52.222–53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).
- (O) 52.222–54, Employment Eligibility Verification (Oct 2015) (Executive Order 12989).
- (P) 52.222–55, Minimum Wages Under Executive Order 13658 (Dec 2015).
- (Q) 52.222–62, Paid sick Leave Under Executive Order 13706 (Jan 2017) (E.O. 13706).
- (R) (1) 52.224–3, Privacy Training (Jan 2017) (5 U.S.C. 552a).
(2) Alternate I (Jan 2017) of 52.224–3
- (S) 52.225–26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).
- (T) 52.226–6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226–6.
- (U) 52.247–64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247–64.

C.3 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

Attachment 1: Install Base Inventories

Attachment 2: Cloud Service Router Inventories

Attachment 3: Pricing Sheet

SECTION E - SOLICITATION PROVISIONS

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

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

<http://www.acquisition.gov/far/index.html>

<http://www.va.gov/oal/library/vaar/>

(End of Provision)

<u>FAR Number</u>	<u>Title</u>	<u>Date</u>
52.209-7	INFORMATION REGARDING RESPONSIBILITY MATTERS	OCT 2018
52.212-1	INSTRUCTIONS TO OFFERORS—COMMERCIAL ITEMS	OCT 2018
52.217-5	EVALUATION OF OPTIONS	JUL 1990

E.2 52.212-3 OFFEROR REPRESENTATIONS AND CERTIFICATIONS—COMMERCIAL ITEMS (OCT 2018)

The Offeror shall complete only paragraph (b) of this provision if the Offeror has completed the annual representations and certification electronically in the System for Award Management (SAM) accessed through <https://www.sam.gov>. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (u) of this provision.

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

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

Forced or indentured child labor means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

Highest-level owner means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

Immediate owner means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

Inverted domestic corporation means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

Manufactured end product means any end product in product and service codes (PSCs) 1000-9999, except—

- (1) PSC 5510, Lumber and Related Basic Wood Materials;
- (2) Product or Service Group (PSG) 87, Agricultural Supplies;
- (3) PSG 88, Live Animals;
- (4) PSG 89, Subsistence;
- (5) PSC 9410, Crude Grades of Plant Materials;
- (6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
- (7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
- (8) PSC 9610, Ores;
- (9) PSC 9620, Minerals, Natural and Synthetic; and
- (10) PSC 9630, Additive Metal Materials.

Place of manufacture means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

Predecessor means an entity that is replaced by a successor and includes any predecessors of the predecessor.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of

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

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

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

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

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

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

(6) Have been voluntarily suspended.

“Sensitive technology”—

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

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

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

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

Service-disabled veteran-owned small business concern—

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

Small disadvantaged business concern, consistent with 13 CFR 124.1002, means a small business concern under the size standard applicable to the acquisition, that—

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by—

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding \$750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

Subsidiary means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

Successor means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term “successor” does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

Veteran-owned small business concern means a small business concern—

(1) Not less than 51 percent of which is owned by one or more veterans (as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

Women-owned business concern means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

Women-owned small business concern means a small business concern—

- (1) That is at least 51 percent owned by one or more women; or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and
- (2) Whose management and daily business operations are controlled by one or more women.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127), means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

(b)(1) Annual Representations and Certifications. Any changes provided by the Offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications in SAM.

(2) The offeror has completed the annual representations and certifications electronically in SAM accessed through <http://www.sam.gov>. After reviewing SAM information, the Offeror verifies by submission of this offer that the representations and certifications currently posted electronically at FAR 52.212–3, Offeror Representations and Certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), at the time this offer is submitted and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs .

(c) Offerors must complete the following representations when the resulting contract will be performed in the United States or its outlying areas. Check all that apply.

(1) *Small business concern.* The offeror represents as part of its offer that it [] is, [] is not a small business concern.

(2) *Veteran-owned small business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it [] is, [] is not a veteran-owned small business concern.

(3) *Service-disabled veteran-owned small business concern.* [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents as part of its offer that it [] is, [] is not a service-disabled veteran-owned small business concern.

(4) *Small disadvantaged business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [] is, [] is not a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) *Women-owned small business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [] is, [] is not a women-owned small business concern.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that—

(i) It ☐ is, ☐ is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It ☐ is, ☐ is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [*The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture: _____.*] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.] The offeror represents that—

(i) It ☐ is, ☐ is not an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It ☐ is, ☐ is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [*The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture: _____.*] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

Note: Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(8) *Women-owned business concern (other than small business concern).* [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it ☐ is a women-owned business concern.

(9) *Tie bid priority for labor surplus area concerns.* If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

(10) *HUBZone small business concern.* [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that—

(i) It ☐ is, ☐ is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material change in ownership and control, principal office, or HUBZone employee percentage has occurred since it was certified by the Small Business Administration in accordance with 13 CFR Part 126; and

(ii) It ☐ is, ☐ is not a joint venture that complies with the requirements of 13 CFR Part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for the HUBZone small business concern or concerns that are participating in the joint venture. [The offeror shall enter the name or names of the HUBZone small business concern or concerns that are participating in the joint venture: _____.] Each HUBZone small business concern participating in the joint venture shall submit a separate signed copy of the HUBZone representation.

(d) Representations required to implement provisions of Executive Order 11246—

(1) *Previous contracts and compliance.* The offeror represents that—

(i) It ☐ has, ☐ has not participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It ☐ has, ☐ has not filed all required compliance reports.

(2) *Affirmative Action Compliance.* The offeror represents that—

(i) It ☐ has developed and has on file, ☐ has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It ☐ has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) *Certification Regarding Payments to Influence Federal Transactions* (31 U.S.C. 1352). (Applies only if the contract is expected to exceed \$150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to

provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) *Buy American Certificate*. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American—Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of “domestic end product.” The terms “commercially available off-the-shelf (COTS) item,” “component,” “domestic end product,” “end product,” “foreign end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American—Supplies.”

(2) Foreign End Products:

Line Item No	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(g)(1) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate*. (Applies only if the clause at FAR 52.225-3, Buy American—Free Trade Agreements—Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms “Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product,” “commercially available off-the-shelf (COTS) item,” “component,” “domestic end product,” “end product,” “foreign end product,” “Free Trade Agreement country,” “Free Trade Agreement country end product,” “Israeli end product,” and “United States” are defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act.”

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or

Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) of this provision) as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act.” The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of “domestic end product.”

Other Foreign End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I.* If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Canadian End Products:

Line Item No.

[List as necessary]

(3) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II.* If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Canadian or Israeli End Products:

Line Item No.	Country of Origin
---------------	-------------------

<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>

[List as necessary]

(4) *Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate III.* If Alternate III to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled “Buy American—Free Trade Agreements—Israeli Trade Act”:

Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.	Country of Origin
---------------	-------------------

<hr/>	<hr/>
<hr/>	<hr/>
<hr/>	<hr/>

[List as necessary]

(5) *Trade Agreements Certificate*. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product, as defined in the clause of this solicitation entitled “Trade Agreements”.

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products:

Line Item No.	Country of Origin
_____	_____
_____	_____
_____	_____

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) *Certification Regarding Responsibility Matters* (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals—

(1) ☐ Are, ☐ are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) ☐ Have, ☐ have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or Commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property;

(3) ☐ Are, ☐ are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) [] Have, [] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds \$3,500 for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) *The tax liability is finally determined.* The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) *The taxpayer is delinquent in making payment.* A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) *Examples.*

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. Sec. 6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. Sec. 6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. Sec. 6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. 362 (the Bankruptcy Code).

(i) *Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126).*

(1) *Listed end products.*

Listed End Product Listed Countries of Origin

(2) *Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(ii) by checking the appropriate block.]*

☐ (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

☐ (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) *Place of manufacture.* (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) ☐ In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) ☐ Outside the United States.

(k) *Certificates regarding exemptions from the application of the Service Contract Labor Standards.* (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) ***[The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]***

☐ (1) Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror ☐ does ☐ does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003- 4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

☐ (2) Certain services as described in FAR 22.1003- 4(d)(1). The offeror ☐ does ☐ does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) *Taxpayer Identification Number (TIN)* (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to SAM to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS).

(2) The TIN may be used by the Government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) *Taxpayer Identification Number (TIN).*

☐ TIN: _____.

☐ TIN has been applied for.

☐ TIN is not required because:

☐ Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

☐ Offeror is an agency or instrumentality of a foreign government;

☐ Offeror is an agency or instrumentality of the Federal Government.

(4) *Type of organization.*

☐ Sole proprietorship;

☐ Partnership;

☐ Corporate entity (not tax-exempt);

☐ Corporate entity (tax-exempt);

☐ Government entity (Federal, State, or local);

☐ Foreign government;

☐ International organization per 26 CFR 1.6049-4;

☐ Other _____.

(5) *Common parent.*

☐ Offeror is not owned or controlled by a common parent;

☐ Name and TIN of common parent:

Name _____.

TIN _____.

(m) *Restricted business operations in Sudan.* By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) *Prohibition on Contracting with Inverted Domestic Corporations.*

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted

domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) *Representation.* The Offeror represents that—

- (i) It [] is, [] is not an inverted domestic corporation; and
- (ii) It [] is, [] is not a subsidiary of an inverted domestic corporation.

(o) *Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.*

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

(2) *Representation and certifications.* Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

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

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds \$3,500 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (see OFAC's Specially Designated Nationals and Blocked Persons List at <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (*e.g.*, 52.212-3(g) or a comparable agency provision); and

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

(p) *Ownership or Control of Offeror.* (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation).

(1) The Offeror represents that it [] has or [] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall

respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates “has” in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code: ____.

Immediate owner legal name: ____.

(Do not use a “doing business as” name)

Is the immediate owner owned or controlled by another entity: ☐ Yes or ☐ No.

(3) If the Offeror indicates “yes” in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest-level owner CAGE code: ____.

Highest-level owner legal name: ____.

(Do not use a “doing business as” name)

(q) Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.

(1) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, The Government will not enter into a contract with any corporation that—

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that—

(i) It is ☐ is not ☐ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed,

and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is ☐ is not ☐ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) *Predecessor of Offeror*. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it ☐ is or ☐ is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated “is” in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code: ____ (or mark “Unknown”).

Predecessor legal name: ____.

(Do not use a “doing business as” name).

(s) [Reserved]

(t) *Public Disclosure of Greenhouse Gas Emissions and Reduction Goals*. Applies in all solicitations that require offerors to register in SAM (12.301(d)(1)).

(1) This representation shall be completed if the Offeror received \$7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than \$7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)]. (i) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible Web site the results of a greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) ☐ does, ☐ does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible Web site a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible Web site includes the Offeror’s own Web site or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked “does” in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible Web site(s) where greenhouse gas emissions and/or reduction goals are reported:_____.

(u)(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) Representation. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(End of Provision)

E.3 52.216-1 TYPE OF CONTRACT (APR 1984)

The Government contemplates award of a Firm-Fixed-Price contract resulting from this solicitation.

(End of Provision)

E.4 52.233-2 SERVICE OF PROTEST (SEP 2006)

Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer (addressed as follows) by obtaining written and dated acknowledgment of receipt from:

Juan Quinones

Contracting Officer
Hand-Carried Address:
Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

Mailing Address:
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of Provision)

E.5 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (OCT 2018)

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

- (1) Include the name, address, fax number, email and telephone number of the protester;
- (2) Identify the solicitation and/or contract number;
- (3) Include an original signed by the protester or the protester's representative and at least one copy;
- (4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;
- (5) Specifically request a ruling of the individual upon whom the protest is served;
- (6) State the form of relief requested; and
- (7) Provide all information establishing the timeliness of the protest.

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

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

(End of Provision)

E.6 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (OCT 2018)

(a) As an alternative to filing a protest with the Contracting Officer, an interested party may file a protest by mail or electronically with: Executive Director, Office of Acquisition and Logistics, Risk Management

and Compliance Service (003A2C), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or Email: *EDProtests@va.gov*.

(b) The protest will not be considered if the interested party has a protest on the same or similar issue(s) pending with the Contracting Officer.

(End of Provision)

E.7 BASIS FOR AWARD

Award will be made to the lowest evaluated priced, technically acceptable proposal. To receive consideration for award, a rating of Acceptable must be achieved for the Technical Factor.

E. 8 FACTORS TO BE EVALUATED

1. Technical
2. Price

E.9 EVALUATION APPROACH

All proposals shall be subject to evaluation by a team of Government personnel. The Government intends to award without discussions based upon the initial evaluation of proposals, as detailed below.

All Offerors are advised that, in the interest of efficiency, the Government reserves the right to conduct the evaluation in the most effective manner. Specifically, the Government may first evaluate the total proposed price of all Offerors. Thereafter, the Government will evaluate the technical proposal of the lowest evaluated priced Offeror, only. If the lowest evaluated priced Offeror's technical proposal is determined to be rated Acceptable, the Government may make award to that Offeror without further evaluation of the remaining Offerors' technical proposals. If the lowest evaluated priced Offeror's technical proposal is determined to be rated either Unacceptable or Susceptible to being made Acceptable, then the Government may evaluate the next lowest evaluated priced technical proposal, and so forth and so on, until the Government reaches the lowest evaluated priced technical proposal that is determined to be rated Acceptable. However, the Government reserves the right to evaluate all Offerors' technical proposals should it desire to conduct discussions, or otherwise determine it to be in the Government's best interest.

The proposal will be evaluated strictly in accordance with its written content. Proposals which merely restate the requirement or state that the requirement will be met, without providing supporting rationale, are not sufficient. Offerors who fail to meet the minimum requirements of the Solicitation will be rated Unacceptable and thus, ineligible for award.

1. TECHNICAL EVALUATION APPROACH: The evaluation process will consider whether the proposal demonstrates a clear understanding of the technical features involved in meeting the solicitation requirements and whether the Offeror's methods and approach have adequately and completely considered, defined and satisfied the requirements in the Solicitation.

2. PRICE EVALUATION APPROACH: The Total Contract Evaluated Price will be the sum of the evaluated FFP line items, including all options. The Government will verify the Offeror's Total Contract Evaluated Price using the Excel Pricing spreadsheet at Attachment 3. The Government will adjust the Offeror's proposed Total Contract Evaluated Price if mathematical errors are identified.

a. FFP: The Total Contract Evaluated FFP will be calculated as follows:

- i. The Government has identified its current Cisco product inventory in the VA Master Inventory List, found at Attachment 002. This inventory is also known as the "Install Base." The Cisco Collaboration Flex Band is based on the initial base quantities as defined in the PWS paragraph 5.4.3. The Government will provide the exact Install Base and Collaboration Flex Band as identified in Attachment 2 and PWS paragraph 5.4.3 for the base period for the calculation of the Base Period Price. The Total Evaluated Base Period Price shall be the sum of the provided Install Base Band, Collaboration Flex Band and not to exceed (NTE) Cisco Learning Credits (CLC).
- ii. To account for fluctuation to VA's Install base and Knowledge Workers (KW), the Government has identified bands for pricing purposes in the option periods. The Government has specified weighted percentages relative to each of the Install Base Bands and Collaboration Flex Bands, which shall be used for evaluation purposes only. Install Base Bands and Collaboration Flex Bands and their relative weightings have been identified for each option period in Attachment 3 – Pricing Sheet. The Offeror's proposed FFP Lot Price for each Install Base Band/ Collaboration Flex Band will be multiplied by the Government-specified weighting. The Offeror's FFP Lot Price multiplied by the Government'-specified weighting shall be known as the "Weighted Price." The sum of Weighted Price for each Install Band shall be known as "Total Install Base Weighted Price". The sum of Weighted Price for each Collaboration Flex Band shall be known as "Total Collaboration Flex Weighted Price". All weighted prices identified within a given line item will be summed to derive the Total Install Base Weighted Price and the Total Collaboration Flex Weighted Price.
- iii. The Total Evaluated Price for each 12-month option period will be calculated by adding the Total Install Base Weighted Price, the Total Collaboration Flex Weighted Price and the NTE CLC price.
- iv. The Total Contract Evaluated Price will then be the sum of the Total Evaluated Base Period Price and the Total Evaluated Price for each Option Period.

The example below shows how the Total Evaluated Price will be computed for a hypothetical line item where the Install Base band pricing is required:

EXAMPLE:

Install Base Evaluated Price Calculation			
Install Base Bands (\$M)	Lot Price	% Weight	Weighted Price
500 - 600	\$700	5%	\$35

600 - 700	\$800	5%	\$40
700 - 800	\$900	5%	\$45
800 - 900	\$1,000	15%	\$150
900 - 1000	\$1,100	20%	\$220
1000 - 1100	\$1,200	20%	\$240
1100 - 1200	\$1,500	15%	\$225
1200 - 1350	\$1,750	10%	\$175
1350 - 1500	\$2,100	5%	\$105
Total Install Base Weighted Price		100%	\$1,235

Collaboration Flex Evaluated Price Calculation			
Knowledge Workers (KW) Units Bands	Lot Price	% Weight	Weighted Price
260,000 - 311,999	\$900	40%	\$35
312,000 - 374,399	\$1000	40%	\$40
374,400 - 449,279	\$1,100	10%	\$220
449,280 - 539,140	\$1,200	10%	\$240
Total Collaboration Flex Weighted Price		100%	\$1,235

Total Evaluated Price Calculation		
Total Install Base Weighted Price	+ Collaboration Flex Service Weighted Price	=Total Evaluated Price
\$1,235	\$1,200	\$2,435

- b. Please be advised that the formulaic evaluation approach delineated above shall be used by the Government for evaluation purposes, only. Therefore, although any award resulting from this Solicitation shall be made based on the total lowest evaluated price which proves to be technically acceptable, the awarded contract price shall be based solely on the successful Offeror's firm-fixed pricing proposed for the Install Base Bands plus the Collaboration Flex Services elected by the Government for the respective period of performance.

E.10 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 three volumes. The Volumes are I – Technical, II – Price, and III - Solicitation, Offer and Award Documents and Certifications/Representations. 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 36C10B19R0043 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 complete 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 complete 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	Tech.pdf	30
Volume II	Price	Price.xls	None (Submit Excel Pricing Spreadsheet)
Volume III	Solicitation, Offer & Award Documents, Certifications & Representations	OfrRep.pdf	None
	Small Business Subcontracting Plan (Large Businesses Only)	SBSP.pdf	None

Any Cover Page, Table of Contents, and/or a glossary of abbreviations or acronyms 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 Federal Acquisition Regulation (FAR) 52.212-1, Instructions to Offerors – Commercial Items.

(i) VOLUME I – TECHNICAL FACTOR

- a. The technical proposal shall demonstrate that the Offeror is fully capable of meeting all tasks of the Performance Work Statement (PWS). Any tasks not specifically referenced below are incorporated into these requirements and should be addressed in the proposal. The Offeror shall propose a detailed approach to:
 - (1) Providing and meeting all required program management requirements as defined in PWS paragraph 5.1 and its subtasks. The Offeror shall demonstrate that its management approach is sufficient to provide the required services across an Enterprise as large, complex and geographically distributed as VA's.
 - (2) Providing SNTC services and support coverage for all VA Cisco assets as provided in Attachment 002 - VA Master Inventory and all services defined in PWS paragraphs 5.2 through 5.2.7. This includes meeting all defined metrics and service level agreements.
 - (3) Providing SWSS for all VA owned and managed Cisco Unified Border Element (CUBE)s and Cisco® Unified Session Initiation Protocol (SIP) Proxy (CUSP) services and annual term renewals for all base, security and other licenses for all VA owned Cisco Cloud Services Router (CSR) 1000V as defined in PWS paragraphs 5.3 and 5.3.1.
 - (4) Providing all Cisco Collaboration Flex Enterprise Service and support to VA for the capabilities and quantities as defined in PWS paragraphs 5.4 through 5.4.3.

(5) Providing all Cisco Business-Critical Services as defined in PWS paragraphs 5.5.1 through 5.5.22.

(6) Providing all required System and Organizational Controls (SOC) for Service Organizations reporting as defined in PWS paragraphs 5.6 through 5.6.2.

b. In addition, the Offeror shall:

(1) Provide a letter signed by an Officer at Cisco and on Cisco Letterhead confirming the Offeror is an authorized Cisco reseller, to include certification level and date including evidence that it is an Advanced Technology Partner (ATP) for the Cisco Unified Contact Center Enterprise (UCCE) platform or has access to a support vendor that has this same ATP certification at time of proposal submission for the duration of this effort. Failure to provide the letter from Cisco confirming that you are an authorized Cisco reseller and are an ATP for Cisco UCCE platform at time of proposal submission will render your proposal Unacceptable and thus ineligible for award.

(ii) VOLUME II – PRICE FACTOR

a. The Offeror shall complete the Schedule of Supplies/Services found in the Excel Pricing Attachment 3 - Pricing Sheet, attached hereto. Breakdown of cost data is not required in as much as the Contracting Officer anticipates adequate price competition.

b. The Offeror shall complete the Excel Pricing Attachment 3 - Pricing Sheet. The Offeror shall input a Lot price for the Base year and input Lot prices for each Install Base Band/Collaboration Flex Band for every item in each of the yellow shaded cells for each option period. Proposed prices shall be no more than two decimal places.

Calculation of the Total Evaluated FFP will be done automatically in the Spreadsheet. The Total Install Base Weighted Price and the Total Collaboration Flex Weighted Price will be calculated based on the LOT prices entered by the Offeror. The spread sheet will sum the Base Period total and the Option Period totals including the Install Base Weighted Price, the Collaboration Flex Weighted Price and the NTE CLC Price to derive the Total Contract Evaluated Price. Please be advised that the Offeror is bound to the firm-fixed pricing proposed for each of the yellow shaded cells.

c. All Offerors should propose using an estimated award date of October 1, 2019.

(iii) VOLUME III - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS

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

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

(2) 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): 5.0% of the total contract value; Veteran-Owned Small Business (VOSB): 7.0% 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.

(3) Any proposed terms and conditions and/or assumptions upon which the proposal is predicated. However, please be advised that any Offeror imposed terms and conditions and/or assumption 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.