AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	84

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
P00001	3/16/16.		NA

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

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
HMS TECHNOLOGIES, INC. 1 DISCOVERY PL MARTINSBURG WV 25403		9B. DATED (SEE ITEM 11)
		10A. MODIFICATION OF CONTRACT/ORDER NO. VA118-16-D-1014
CODE 3UXA1 FACILITY CODE	X	10B. DATED (SEE ITEM 13) 03-07-2016

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

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

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

12. ACCOUNTING AND APPROPRIATION DATA (If required)

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

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

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

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

See Continuation Page(s)

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

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)
Roy H. jones, Jr. - VP of Contracts	Matthew Ginty Contracting Officer
15B. CONTRACTOR/OFFEROR Roy H. Jones Jr (Signature of person authorized to sign)	15C. DATE SIGNED 3/16/2016
16B. UNITED STATES OF AMERICA BY (Signature of Contracting Officer)	16C. DATE SIGNED 3/16/16.

NSN 7540-01-152-8070
PREVIOUS EDITION NOT USABLE

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA - FAR (48 CFR) 53.243

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	84

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO.(If applicable)
P00001			NA

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

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NO.
HMS TECHNOLOGIES, INC. 1 DISCOVERY PL MARTINSBURG WV 25403		9B. DATED (SEE ITEM 11)
		10A. MODIFICATION OF CONTRACT/ORDER NO. VA118-16-D-1014
CODE 3UXA1 FACILITY CODE	X	10B. DATED (SEE ITEM 13) 03-07-2016

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

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

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

12. ACCOUNTING AND APPROPRIATION DATA (If required)

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

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

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

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

See Continuation Page(s)

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

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

CONTINUATION PAGE:

1. The purpose of this modification P00001 is to:

    a. Incorporate a revised Governing Law Clause at Section B.1.
    b. Incorporate a revised Price Schedule at Section B.3 to include Contract Line Item Numbers (CLIN) 0011 and 1011, Final Section 508 Compliance Test Results.
    c. Incorporate a revised Performance Work Statement (PWS), dated March 10, 2016 at Section C. This PWS, dated March 10, 2016, supersedes the previous PWS, dated November 25, 2014. Reference the PWS Version History table on page # 14 for a description of the changes.
    d. Incorporate revised Clause H.9 Metrics at Section H.
    e. Incorporate Clause H.12, Notification of Satisfaction Survey: Acquisition 360 (July 2015), at Section H.
    f. Incorporate FAR Clause, 52.203-99, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements (DEVIATION 2015-02)
    g. Incorporate FAR Clause 52.209-10, Prohibition on Contracting With Inverted Domestic Corporations (NOV 2015)
    h. Incorporate revised FAR clause 52.216-22, Indefinite Quantity.
    i. Replace FAR clause 52.222-99, Establishing a Minimum Wage for Contractors (DEVIATION) (July 2014) with FAR 52.222-55, Minimum Wages Under Executive Order 13658 (DEC 2014) at Section I.
    j. Incorporate FAR Clause 52.232-39, Unenforceability of Unauthorized Obligations (JUN 2013) at Section I.
    k. Incorporate revised 508 compliant Attachments 3 to 11 at Section J.

2. The revised contract sections above are included within this modification. It is the responsibility of the contractor to review the entirety of the revisions incorporated within this modification.

3. Except as provided herein, all other terms and conditions of this contract remain unchanged and in full force and effect.

SECTION B - SUPPLIES OR SERVICES AND PRICE/COSTS

B.1 GOVERNING LAW

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

B.3 PRICE SCHEDULE

The deliverables associated with Contract Line Item Numbers (CLIN) 0004 through 0011 shall be submitted for each task order and included in the price/cost of each task order. The specific deliverables under CLINs 0004 through 0011 will not be set forth under individual Task Orders.

PRICE SCHEDULE					
BASE PERIOD					
CLIN	**DESCRIPTION**	**QUANTITY**	**UNIT**	**UNIT COSTS**	**TOTAL COST**
0001	**Firm-Fixed-Price Line Item** SECURITY CLASS: Determined at Task Order Level This CLIN is to provide Information Technology (IT) services and incidental supplies on a FFP basis for a period of 60 months from date of award in accordance with (IAW) the Transformation Twenty-One Total Technology Next Generation (T4NG) Performance Work Statement (PWS) set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and Free on Board (FOB) Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
0002	**Time-and-Materials/Labor-Hour Line Item** SECURITY CLASS: Determined at				

	Task Order Level This CLIN is to provide IT services and incidental supplies on a T&M/LH basis for a period of 60 months from date of award IAW the T4NG PWS set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and FOB Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
0003	**<u>Cost Reimbursement Line Item</u>** SECURITY CLASS: Determined at Task Order Level This CLIN is to provide IT services and incidental supplies on a CR basis for a period of 60 months from date of award IAW the T4NG PWS set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and FOB Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
0004	**<u>Contractor's Progress, Status, and Management Report</u>** Monthly Status Report shall be			NSP	NSP

	provided IAW Section C, PWS, Paragraph 8.1.1(A) and (B)(C)(D) and (E), and Section J Attachment 003 when applicable to Task Order contract type. FOB Point: Destination Inspection/Acceptance: Destination				
0005	**<u>Contract Performance Report</u>** Contract Performance Report shall be provided IAW Section C, PWS, Paragraph 8.1.2 (A) and (B), and Section J Attachments 004 (T&M) and 005 (CR) when applicable to Task Order contract type. Report not applicable for FFP Task Orders. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
0006	**<u>Government Furnished Equipment Status Report</u>** Government Furnished Equipment Status Report shall be provided IAW Section C, PWS, Paragraph 8.1.3 (A-K) and Section J, Attachment 006. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
0007	**<u>Personnel Contractor Manpower Report</u>** Personnel Contractor Manpower Report shall be provided IAW Section C, PWS, Paragraph 8.1.4 (A-S) and Section J, Attachments 007 and 008. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP

0008	**Contractor Staff Roster** Contractor Staff Roster shall be provided IAW Section C, PWS, Paragraph 8.1.5 and Section J, Attachment 009. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
0009	**Small Business Participation Report** Small Business Participation Report shall be provided IAW Section H, clause H.4 Small Business Participation Requirements, PWS Paragraph 8.1.6 and Section J, Attachment 010. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
0010	**Veterans Employment Certification Report** Veterans Employment Certification Report IAW Section H, clause H.5, PWS Paragraph 8.1.7 and Section J, Attachment 011. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
0011	**Final Section 508 Compliance Test Results** Final Section 508 Compliance Test Results IAW PWS Paragraph 8.1, Reporting Requirements. FOB Point: Destination Inspection/Acceptance: Destination				

Option Period One

This 60-month option period may be exercised at the Government's discretion IAW FAR 52.217-9, Option to Extend the Term of the Contract (MAR 2000). Work shall not commence until, and unless, a formal modification is issued by the Contracting Officer (CO). If exercised, this option shall commence immediately after expiration of the base period.

PRICE SCHEDULE					
OPTION PERIOD					
CLIN	**DESCRIPTION**	**QUANTITY**	**UNIT**	**UNIT COSTS**	**TOTAL COST**
1001	**Firm-Fixed-Price Line Item** SECURITY CLASS: Determined at Task Order Level This CLIN is to provide IT services and incidental supplies on a FFP basis for a period of 60 months from date of option exercise IAW the T4NG PWS set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and Free on Board (FOB) Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
1002	**Time-and-Materials/Labor-Hour Line Item** SECURITY CLASS: Determined at Task Order Level This CLIN is to provide IT services and incidental supplies on a T&M/LH basis				

	for a period of 60 months from date of option exercise IAW the T4NG PWS set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and FOB Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
1003	**<u>Cost Reimbursement Line Item</u>** SECURITY CLASS: Determined at Task Order Level This CLIN is to provide IT services and incidental supplies on a CR basis for a period of 60 months from date of option exercise IAW the T4NG PWS set forth in Section C. Specific requirements and pricing shall be set forth under individual Task Orders. Inspection, Acceptance, and FOB Point shall be specified by incorporating the appropriate clauses from Sections E and F on each individual Task Order. The delivery or performance schedule shall be determined on each individual Task Order.				
1004	**<u>Contractor's Progress, Status, and Management Report</u>** Monthly Status Report shall be provided IAW Section C, PWS, Paragraph 8.1.1(A) and (B)(C)(D) and (E), and Section J Attachment 003 when applicable to Task Order contract type.			NSP	NSP

	FOB Point: Destination Inspection/Acceptance: Destination				
1005	**Contract Performance Report** Contract Performance Report shall be provided IAW Section C, PWS, Paragraph 8.1.2 (A) and (B), and Section J Attachments 004 (T&M) and 005 (CR) when applicable to Task Order contract type. Report not applicable for FFP Task Orders. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
1006	**Government Furnished Equipment Status Report** Government Furnished Equipment Status Report shall be provided IAW Section C, PWS, Paragraph 8.1.3 (A-K) and Section J, Attachment 006. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
1007	**Personnel Contractor Manpower Report** Personnel Contractor Manpower Report shall be provided IAW Section C, PWS, Paragraph 8.1.4 (A-S) and Section J, Attachments 007 and 008. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
1008	**Contractor Staff Roster** Contractor Staff Roster shall be provided IAW Section C, PWS, Paragraph 8.1.5 and Section J, Attachment 009. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP

1009	**Small Business Participation Report** Small Business Participation Report shall be provided IAW Section H, clause H.4 Small Business Participation Requirements, PWS Paragraph 8.1.6 and Section J, Attachment 010. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
1010	**Veterans Employment Certification Report** Veterans Employment Certification Report IAW Section H, clause H.5, PWS Paragraph 8.1.7 and Section J, Attachment 011. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP
1011	**Final Section 508 Compliance Test Results** Final Section 508 Compliance Test Results IAW PWS Paragraph 8.1, Reporting Requirements. FOB Point: Destination Inspection/Acceptance: Destination			NSP	NSP

Contract Maximum/Minimum Ceiling:

IAW Section I, clause 52.216-22 entitled, "Indefinite Quantity" the Maximum value of the T4NG contract is $22.3 Billion. The maximum overall value of the T4NG contract for both the base period and options is $22.3 Billion. The maximum overall value of the base period is $10.4B. The maximum value of the T4NG contract in the option period, if exercised, is $11.9B. IAW Section I, clause 52.216-22 entitled, "Indefinite Quantity" the Minimum guaranteed value under the T4NG contract is $500,000. The Government reserves the right to award initial orders at the time of the basic contract award on a sole source basis pursuant to FAR 16.505(b)(2)(iv) at amounts which may exceed the minimum guaranteed value. There will be no guaranteed minimum order for the option period, if exercised.

The ceiling price as set forth in Section I, clause 52.232-7 entitled, "Payments under Time-and-Materials and Labor-Hour contracts" will be established for each individual Time-and Materials Task Order.

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

Performance Work Statement (PWS)
for the

Transformation Twenty-One Total Technology
Next Generation (T4NG)
Program

DATE: March 10, 2016

Department of Veterans Affairs
Office of Acquisition Operations (OAO)
Technology Acquisition Center (TAC)

Version #	Version Description	Release Date
2.0	1. Section 2.0, changed previous reference list using "letters" to a "numbered" list 2. Section 2.0, #21, VA Handbook 6500 reference updated 3. Section 2.0, #22 Revised VA Handbook 6500.1 release date 4. Section 2.0, updated #29, to include new link for ProPath Processes and Templates 5. Section 2.0, #33 Added One-VA to the title of TRM 6. Section 2.0, Removed duplicate reference to Directive 6300, now #37 only 7. Section 2.0, #59 Updated TIC reference and link 8. Section 2.0, Added #70, "Remote Access" OIS Memorandum reference 9. Section 2.0, Added #71, Clinger Cohen Act 10. Section 2.0, Added #72, VA Directive 6071, PMAS 11. Section 2.0 Added #73, #74, #75, VA Memorandums regarding access to VA Information systems using PIV 12. Section 3.6.2, added reference to A3.0 regarding Contractor acquired equipment delivered to the Government 13. Section 3.8, Updated PIV Authentication Language 14. Section 3.8, Updated VA standard computer configuration language for IE11 (James Babe, Kevin Overholt) 15. Section 3.8, Updated broken link to TIC Reference Architecture 16. Section 4.1.6,Program Management Support, added item J, Organizational Change Management 17. Section 6.3, Revised entire Section regarding Remote Access 18. Section 7.1.1 removed requirement regarding PAP 19. Section 8.1, added language regarding Section 508 and deliverables 20. Section 8.1.1 A, added new item #7 regarding Section 508 conformance status reporting for EIT Deliverables for each TO 21. Section 8.1.6, new section added regarding Small	March 10, 2016

Version #	Version Description	Release Date
	Business Participation 22. Section 8.2.3, removed reference to quarterly 23. Section A3.0, fixed broken Section 508 links 24. Section A6.0 Spelled out FEMP acronym, and in paragraph 2 updated broken links 25. Addendum B, reformatted to match lettering/numbering schema in the VA Handbook 26. Addendum B3.0 para 7, BAA Handbook number updated 27. Section B4.0 paragraph 1 and B5.0 paragraph a, Added reference to the TIC Reference Architecture. (Charles Walker, VA NSOC) 28. Accessibility Checker used to ensure Section 508 compliancy, modifications made accordingly and using best practices for Section 508 accessibility in regard to this PWS Template	
1.0	Initial Release	November 7, 2014

1.0 SCOPE

This PWS establishes the requirements for Contractor-provided solutions in support of IT. Contractor-provided solutions may support the Department of Veterans Affairs (VA) and other Federal Agencies. The Contractor shall provide total IT services solutions including the following functional areas: program management, strategy, enterprise architecture and planning; systems/software engineering; software technology demonstration and transition; test and evaluation; independent verification and validation; enterprise network; enterprise management framework; operations and maintenance; cybersecurity; training; IT facilities; and other solutions encompassing the entire range of IT and Health IT requirements, to include software and hardware incidental to the solution. Accordingly, Task Orders may include acquisitions of software and IT products. T4NG is not intended as a mechanism to solely purchase IT products. Such products may be purchased to the extent that those products are necessary to deliver the solution required. These services, as well as related IT products, may encompass the entire life-cycle of a system. Moreover, services and related products covered under this contract shall be global in reach and the Contractors must be prepared to provide services and deliverables worldwide.

This PWS provides general requirements. Specific requirements shall be defined in individual Task Orders. Functional area requirements are described in Section 4.0 and are not mutually exclusive for Task Order requirements. Requirements may fall within one specific functional area but in many cases, the requirements will encompass and apply across and within multiple functional areas to provide the total life cycle solution.

2.0 APPLICABLE DOCUMENTS

The Contractor shall comply with the documents listed below. Additional documents may be listed in individual Task Orders.

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
5. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, title IX Information Security Matters
6. 10 U.S.C. § 2224, "Defense Information Assurance Program"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. Department of Veterans Affairs (VA) Directive and Handbook 0710 Personnel Suitability and Security Program dated May 18, 2007 (http://www1.va.gov/vapubs/)
9. VA Directive 6102 (Internet/Intranet Services), July 15, 2008 (http://www1.va.gov/vapubs/)
10. VA Handbook 6102 (Internet/Intranet Services), July 15, 2008 (http://www1.va.gov/vapubs/)
11. Health Insurance Portability and Accountability Act (HIPAA); 45 CFR Part 160, 162, and 164; Health Insurance Reform: Security Standards; Final Rule dated February 20, 2003
12. VHA Handbook 1605.05, Business Associate Agreements, July 22, 2014(http://www.va.gov/vhapublications/)
13. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
14. Office of Management and Budget Circular A-130, "Management of Federal Information Resources', November 28, 2000
15. U.S.C. Section 552a, as amended
16. Title 32 CFR 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
17. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. Section § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012 (http://www1.va.gov/vapubs/)
21. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015 (http://www1.va.gov/vapubs/)
22. VA Handbook 6500.1, "Electronic Media Sanitization," November 3, 2008 (http://www1.va.gov/vapubs/)
23. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012 (http://www1.va.gov/vapubs/)

24. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014 (http://www1.va.gov/vapubs/)
25. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle," March 22, 2010
26. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle," March 22, 2010 (http://www1.va.gov/vapubs/)
27. VA Handbook 6500.6, "Contract Security," March 12, 2010 (http://www1.va.gov/vapubs/)
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011 (http://www1.va.gov/vapubs/)
29. Office of Information and Technology (OI&T) ProPath Process Methodology (reference process maps at http://www.va.gov/PROPATH/Maps.asp and templates at http://www.va.gov/PROPATH/Templates.asp). NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
30. National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" (http://csrc.nist.gov/publications/PubsSPs.html)
31. Project Management Accountability System (PMAS) portal (http://www1.va.gov/vapubs/)
32. Federal Travel Regulation (FTR) (www.gsa.gov/federaltravelregulation)
33. One-VA Technical Reference Model (TRM) (http://www.va.gov/trm/TRMHomePage.asp)
34. Federal Segment Architecture Methodology (FSAM) v1.0, December 2008
35. National Institute Standards and Technology (NIST) Special Publications 800 series
36. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008 (http://www1.va.gov/vapubs/)
37. VA Directive 6300, Records and Information Management, February 26, 2009 (http://www1.va.gov/vapubs/)
38. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010 (http://www1.va.gov/vapubs/)
39. OMB Memorandum, "Transition to IPv6", September 28, 2010
40. OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" December 8, 2011 (FedRAMP Policy Memorandum)
41. VA Directive 6609, "Mailing of Sensitive Personal Information", May 20, 2011 (http://www1.va.gov/vapubs/)
42. OneVA Enterprise Technology Strategic Plan, February 28, 2014
43. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011 (http://www1.va.gov/vapubs/)
44. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014 (http://www1.va.gov/vapubs/)
45. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
46. 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

47. 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
48. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
49. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
50. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
51. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
52. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
53. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
54. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
55. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
56. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
57. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
58. IAM Identity Management Business Requirements Guidance document, May 2013, (https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
59. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
60. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
61. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
62. 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)
63. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
64. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
65. Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," October 5, 2009
66. Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," January 24, 2007
67. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001

68. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013 (http://www1.va.gov/vapubs/)
69. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013 (http://www1.va.gov/vapubs/)
70. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
71. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
72. VA Directive 6071, Project Management Accountability System (PMAS), February 20, 2013
73. 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
74. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ#7613595), June30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
75. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ#7613597), June30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

3.0 GENERAL REQUIREMENTS

The Contractor shall provide and/or acquire the services, hardware, and software required by individual Task Orders pursuant to the general requirements specified below.

3.1 CONTRACT TYPE

This is an Indefinite Delivery/Indefinite Quantity (IDIQ) Multiple Award Task Order (MATO) contract. Individual Task Orders shall be issued on a performance-based T&M, CR, and/or FFP basis.

3.2 ORDERING PERIOD

The ordering period for the basic contract shall be five years with one five-year option.

3.3 HOURS OF WORK

Work at a Government site shall not take place on Federal holidays or weekends unless directed by the CO. The Contractor may also be required to support 24/7 operations 365 days per year as identified in individual Task Orders.

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

Under current definitions, four are set by date:

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

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

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

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

3.4 PLACE OF PERFORMANCE

The place of performance shall be identified in individual Task Orders. Locations will be Government or non-Government sites within the continental United States (CONUS) and/or outside the continental United States (OCONUS). Locations may include but are not limited to Federal, State, VA, or military data centers, facilities, regional offices, benefits delivery centers, medical treatment facilities, health clinics and Tricare facilities as defined in individual Task Orders.

3.5 TRAVEL

Travel shall be IAW individual Task Order requirements. Travel details must be provided to and approved by the CO's Representative (COR) or the Government designee prior to the commencement of travel. All travel shall be IAW the Federal Travel Regulations (FTR). OCONUS travel may require additional authorization and approvals as specified in the individual Task Order.

3.6 MATERIALS, EQUIPMENT AND LOCATIONS

3.6.1 Government-Furnished

Government Furnished Property (GFP) which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and Government Furnished Equipment (GFE) may be provided and shall be identified in the individual Task Order. The Contractor shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt. The Contractor shall be responsible for reporting all inspection results, maintenance actions, losses, and damage to the Government through the VA Technology Acquisition Center (TAC) website.

VA may provide VA specific software as appropriate and required in individual Task Orders. The Contractor may utilize VA provided software development and test accounts, document and requirements repositories and others as required for the development, storage, maintenance and delivery of products. Contractors shall comply with VA security policies and procedures with respect to protecting sensitive data. See Section 6.0 for detailed security requirements.

3.6.2 Contractor-Acquired

The Contractor shall acquire and/or provide any hardware and/or software required to accomplish each Task Order that is not provided as GFP. Software integrity shall be maintained by the Contractor within the licensing agreement of the producer until such software is delivered to the Government, or otherwise disposed of IAW Government direction. Items delivered to the Government shall be approved by the Government in advance of purchase and shall be in compliance with PWS paragraphs 3.8 and A3.0. See Section 6.0 for detailed security requirements.

3.6.3 Non-Developmental Items and Commercial Processes

Non-Developmental Items (NDI), Commercial-Off-The-Shelf (COTS) and Government-Off-The-Shelf (GOTS) products shall be used to the maximum extent. The Contractor shall apply commercially available and industry best processes, standards and technologies to the maximum extent.

3.6.4 Connectivity

VA will provide connectivity to VA specific systems/network as required for execution of the task via VA approved remote access technology. Currently this may include but is not limited to Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE). This remote access will provide connectivity to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. VA may install equipment at the Contractor's site to ensure security requirements are in place. The Contractor must meet the requirements of VA Handbook 6500 and will bear the cost to provide connectivity to VA. Other connectivity to VA systems may be authorized as appropriate in individual Task Orders.

3.6.5 Facilities

Work may be performed at either a Government or non-Government facility. Each Task Order shall delineate the location requirements.

3.6.5.1 Government Facilities

Certain Government office or laboratory space may be made available for performance of individual Task Orders. Contractors may be required to establish operations and support Government locations and shall comply with VA and/or Federal assessment and authorization (A&A) requirements. Such facilities shall be specified in the individual Task Order.

3.6.5.2 Non-Government Facilities

Personnel may perform at Contractor or remote facilities if specified in the individual task order. Contractors may be required to establish operations and support Contractor facilities and shall comply with VA and/or Federal A&A requirements. Such facilities shall be specified in the individual Task Order. The Contractor shall disclose specific facility information during the Request for Task Execution Plan (RTEP) process. All facilities shall be approved by VA and in compliance with PWS paragraph 6.0, Security and Privacy.

3.6.6 Warranty

Items acquired under this contract may require warranty protection. Commercial warranties shall be transferred to the Government. The type of warranty and extent of coverage shall be determined on an individual Task Order basis.

3.6.7 Marking, Handling, Storage, Preservation, Packaging, Tracking & Shipping

The Contractor shall establish/maintain procedures IAW VA Handbook 6500 and VA Directive 6609 for handling, storage, preservation, packaging, marking, tracking and shipping to protect the quality of products and prevent damage, loss, deterioration, degradation or substitution of products.

3.6.8 Export Control

The Contractor shall comply with all applicable laws and regulations regarding export-controlled information and technology and shall not use, distribute, transfer or transmit technology (even if incorporated into products, software or other information) except in compliance with such laws and regulations. In addition, the Contractor shall plan for, obtain, and maintain any and all export licensing required to satisfy individual Task Order requirements.

3.7 SAFETY AND ENVIRONMENTAL

Safety and environmental procedures shall be identified in individual Task Order requirements.

The Contractor shall comply with the Office of Federal Procurement Policy Green Acquisition initiatives as identified in individual Task Orders IAW the policies referenced at http://www.whitehouse.gov/omb/procurement_index_green.

3.8 ENTERPRISE AND IT FRAMEWORK

For VA specific task orders, the Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM) and consider the OneVA Enterprise Technology Strategic Plan. One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the IT used to develop, operate, and maintain enterprise applications.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, “VA System Security

Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications.

The Contractor solution shall support Internet Protocol Version 6 (IPv6) in accordance with the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf), August 2, 2005 http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf), and (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: Technical Infrastructure for USGv6 Adoption" (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support dual stack 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 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies, which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (https://www.fedramp.gov/files/2015/04/TIC_Ref_Arch_v2-0_2013.pdf).

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013, and

Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013, and Windows 8.1 individually as the VA standard, Office 2013, and Windows 8.1 will supersede Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Enterprise Management Framework (EMF) provides an enterprise-wide view of VA IT systems comprised of tools, reports, databases, dashboards, and analytics. EMF enables OI&T to view the health and performance of systems and provides intelligent analysis and trending that enables proactive enterprise system management. Performance, availability, user experience and reliability of IT service delivery is improved as OI&T is able to make strategic, operational and investment decisions based on real-time information.
EMF supports a unified enterprise service management model including release management, configuration management, change management, and incident management aligned with industry standard IT Infrastructure Library (ITIL) service management best practices. The EMF Federated Data Repository (FDR) includes the implementation of a foundational component. The EMF FDR is a national repository that collects enterprise IT management data from VA Managed Data Repositories (MDRs) and integrates with existing VA monitoring and performance systems.

Additional frameworks may be specified in individual task orders.

3.9 DEVELOPMENT METHODOLOGIES

The Contractor may support a Service-Oriented Architecture (SOA) that is a flexible set of design principles used during the phases of systems development and integration which will be specified at the task order level. The deployed SOA-based architecture will be deployed on a secure, scalable, interoperable and dynamic platform that has the end to end visibility and manageability from application services to the networking components level and that can be used within multiple domains.

For VA specific task orders, the Contractor shall support VA efforts IAW the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide mandate to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

For VA specific task orders, the Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

The Contractor shall use an incremental development methodology such as Agile unless otherwise specified at the task order level.

3.10 INTERGRATED PRODUCT TEAMS

The Contractor may be required to serve as a member of, or provide Subject Matter Expertise to Integrated Product Teams (IPTs) or Integrated Business Teams (IBTs) within VA. Their role(s) will be identified in individual Task Orders. IPTs and IBTs are cross-functional teams that work collaboratively to develop strategies and approaches to meet particular objectives. IPTs and IBTs bring together the principal stakeholders and focus efforts on establishing critical elements of all phases of the acquisition lifecycle.

3.11 QUALITY ASSURANCE

If a Contractor is required to develop a significant portion of any mission critical systems/software product under this contract, the Contractor may be required to demonstrate they, or the Subcontractor performing the task, are operating at a specified Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration (CMMI) for Development (CMMI-DEV) level; CMMI for Acquisition (CMMI-ACQ) level; CMMI for Services (CMMI-SVC) level; and/or International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 20000, Institute of Electrical and Electronics Engineers (IEEE) 1012, or ISO 9001:2008, ITIL 2011).

If required at the Task Order level, the rating of CMMI Level III or below shall be stated as well as the date of the rating, the identification of the rating organization, the projects/divisions that were evaluated as part of the evaluation and the rating achieved by the specific business unit the Contractor is proposing on systems/software efforts. The Government reserves the right to validate the systems/software developers' process assertions and representations by conducting an evaluation by VA or a third party or appraisals of the Contractor's organization and Subcontractors using commonly accepted Industry/Government validation practices.

3.12 TRANSITION AND ORIENTATION SUPPORT

The Contractor shall perform transition and orientation services (e.g. develop Phase-In/Phase-Out Transition Plan) to insure continuity of services as specified in the individual Task Order. Transition and orientation support may include transitioning support services to Government or Contractor personnel.

3.13 GOVERNMENT INSPECTION AND OVERSIGHT

The Contractor shall cooperate with authorized Government offices in the areas of facilities access, audits, security incident notification, and hosting location.
Specifically, the Contractor (and any Subcontractors) shall:

a. Provide the CO, designated representative of the CO, and representatives of authorized Government offices, full and free physical and remote/logical access to the Contractor's (and Subcontractors') facilities, installations, operations documentation, databases, and personnel used for contract hosting services. This access shall be provided to the extent required to carry out audits, inspections, device scanning utilizing Government prescribed tools, investigations, or other reviews to ensure compliance with contractual requirements for IT and information security, and to safeguard against threats and hazards to the integrity, availability, and confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor)
b. Fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the CO or other authorized Government offices as described in subparagraph (a). Full cooperation includes, but is not limited to, prompt disclosure (per agency policy) to authorized requests of data, information, and records requested in connection with any audit, inspection, investigation, or review, making employees of the Contractor available for interview by auditors, inspectors, and investigators upon request, and providing prompt access (per agency policy) to Contractor facilities, systems, data and personnel to the extent the auditors, inspectors, and investigators reasonably believe necessary to complete the audit, inspection, investigation, or other review. The Contractor's (and any Subcontractors') cooperation with audits, inspections, investigations, and reviews conducted under this clause will be provided at no additional cost to the Government
c. Preserve such data, records, logs and other evidence which are reasonably necessary to conduct a thorough investigation of any computer security incident. A computer security incident (as defined in NIST SP 800-61, Computer Security Incident Handling Guide), including but not limited to, those constituting an actual or potential threat or hazard to the integrity, availability, or confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor), or to the function of information systems operated by the Contractor (or Subcontractor) in the performance of this contract
d. Promptly notify the designated agency representative in the event of any computer security and privacy incident as described in paragraph (c) above. This notification requirement is in addition to any other notification requirements which may be required by law or this contract. Established Federal agency timeframes for reporting security and privacy incidents to the United States Computer Emergency Readiness Team (US-CERT), although not exhaustive, serve as a useful guideline for determining whether reports under this paragraph are made promptly. (See NIST SP 800-61, Computer Security Incident Handling Guide, Appendix J)
e. Provide to the requestor (CO, a representative of the CO, or authorized Government offices) Government data, information, or records under the control of or in the possession of the Contractor pursuant to this contract, which the Agency or authorized Government offices, including the Office of Inspector General, may request in furtherance of other audits, inspections, investigations, reviews or litigation in which the Agency or other authorized Government offices are involved in the form specified at the task order level. Requests for production under this paragraph shall specify a deadline not less than 10 days for compliance which will determine whether response to the request has been made in a timely manner. Unless expressly provided otherwise

elsewhere in this contract, the production of data, information, or records under this paragraph will be at no additional cost to the Government

f. Include the substance of this Section, including this paragraph (f) in any subcontract which would require or otherwise result in Subcontractor employees having access to agency information in the possession or under the control of the Contractor (or Subcontractor), or access to information systems operated by the Contractor (or Subcontractor) in the performance of this contract
g. Ensure that all hosting services pertaining to this contract are performed within the United States of America, including the storage of agency data, information, and records under the control of or in the possession of the Contractor pursuant to this contract

4.0 TECHNICAL FUNCTIONAL AREAS

Individual Task Orders may encompass more than one functional area listed below. Further functional area details are described to provide greater insight into the complexity and uniqueness of some potential Task Order requirements covered by this PWS. Functional area requirements are not mutually exclusive and may apply across multiple functional areas. Efforts to be performed by the Contractor under this contract are of such a nature that they may create a potential organizational conflict of interest as contemplated by Subpart 9.5 of the Federal Acquisition Regulation (FAR). Contractor personnel may be required to sign a non-disclosure agreement.

4.1 PROGRAM MANAGEMENT, STRATEGY, ENTERPRISE ARCHITECTURE AND PLANNING SUPPORT

The Contractor shall provide Program and Project Management, monitoring and analysis, strategy, enterprise architecture and planning support on an enterprise or individual project level. Program Management support is critical to the organization achieving strategic goals and fulfilling mission requirements within programmatic constraints.

4.1.1 Strategy and Planning

The Contractor shall provide services that facilitate strategic decisions for an organization with respect to its current and future IT structure and program integration. This includes conducting a systematic assessment and redesign of the key technologies, business processes, activity-based costing and organizational structures; streamlining processes, properly aligning the organization to reflect the way work gets done, and deploying proven supporting technologies where appropriate. The outcome of future studies and assessments may contribute to an overarching IT strategy, aligned with business goals, objectives, and healthcare and benefits initiatives that leverage innovation to define new opportunities for success. The outcome of studies and assessments may also serve as a critical input into designing a set of metrics, which are measureable objectives related to the overall IT strategy and operations. All recommendations and plans must comply with Federal legislation and be consistent with Federal policy, standards, and guidelines such as: the Government Performance and Results Act, Clinger-Cohen, the Federal Activities Inventory Reform Act, the Paperwork Elimination Act, among others.

4.1.2 Standards, Policy, Procedure and Process Development, and Implementation Support

The Contractor shall provide support in the development/and or evaluation of new Standards, Policy Directives, Operating Procedures, Processes and/or assessments on their impacts when implemented.

4.1.3 Requirements Development and Analysis Support

The Contractor shall provide requirements development support as required by individual Task Orders. Requirements associated with iterative methodologies may occur at any phase of the development lifecycle. Therefore, requirements definition shall be structured to meet the incremental delivery needs of a particular project or program. Requirements support may include, but is not limited to:

A. Enterprise analysis
B. Business and Application architecture
C. Business Process Reengineering
D. Feasibility studies
E. Requirements planning and management
F. Requirements gathering
G. Use Case development
H. Agile requirements methods
I. Requirements analysis
J. Change management
K. Peer Reviews
L. Solution Assessment and Validation
M. Business Process Modeling and workflow management

4.1.3.1 Requirements Packages

The Contractor shall provide requirements package support that may include, but is not limited to:

A. Assistance in developing Statements of Objectives, Statements of Work, PWSs, Performance Specifications, Rough Orders of Magnitude (ROM), cost estimates, Quality Assurance Surveillance Plans, and associated acquisition documentation
B. Technical advice and assistance regarding proposal evaluation
C. Market research, evaluation, and recommendations of technical alternatives

4.1.4 Technology Refresh and Configuration Reviews

The Contractor shall perform technology refresh and configuration reviews to include any structure or process for realizing innovations that provides for business or technical changes. Technology refresh allows for upgrading technology or improving processes as well as helping enterprises move their businesses forward by adopting formal procedures to manage business and technical innovations. Technology refresh ensures new innovations are reviewed and adopted as required. The Contractor shall provide appropriate domain specific recommendations commensurate with unique organizational requirements.

4.1.5 Studies and Analyses

The Contractor shall perform studies and analyses. Such studies/analyses may include, but are not limited to logistics/supportability, engineering, financial, operational, business processes, healthcare and benefits systems and applications to include mobile applications, healthcare and benefits analytics, modernization of existing systems and applications (e.g. VistA), and interoperability and/or information sharing of healthcare and benefits systems across Federal agencies as well as public and private healthcare and benefits systems. The Contractor shall perform non-recurring engineering studies and analyses to evaluate the viability of potential solutions, alternatives to various technical issues and challenges, and emerging products or technology. The Contractor shall perform the evaluation of unproven technology applications and identification of potential risks. The development of pre-production or COTS-based prototypes may be required.

4.1.6 Program Management Support

The Contractor shall provide program management support to accomplish the administrative, managerial, logistical, integration and financial aspects (Program, Planning, Budget and Execution (PPBE)) specified in individual task orders. The Contractor shall identify an individual as the primary contact point for all programmatic issues/concerns/status. The Contractor may be required to provide subject matter expertise to coach, mentor and/or consult with Government Program Managers to plan and execute the processes prescribed by industry and government best practices consistent with organizational policies and procedures as specified in individual Task Orders. For VA specific task orders, the Contractor shall support VA efforts IAW PMAS that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. The Contractor shall support project management functions and reporting which include, but are not limited to:

A. Project Planning
B. Schedule Management
C. Financial Management
D. Earned Value Management (EVM)
E. Quality Management
F. Resource Management
G. Requirements Management
H. Communications Management
I. Project Change Management
J. Organizational Change Management
K. Risk Management
L. Performance Management
M. Knowledge Management (KM)

4.1.7 Product Data

The Contractor shall review, develop and/or submit Product Data that shall be identified in individual Task Orders as deliverables. Product Data may define configuration items, associated processes and procedures, and other items throughout the applicable life cycle. Various types of Product Data, include but are not limited to, engineering drawings, form, fit and function requirements, design documentation, specifications, software configuration documentation,

software code, interface control documentation, Management/project Plans, reports and analyses, PMAS artifacts, quality assurance provisions, and/or commercial item descriptions may be required. The Contractor may be required to apply Computer-Aided Design (CAD), and Computer Automated Engineering (CAE) methods/systems to support concurrent design integration with manufacturing and logistics considerations.

4.1.8 IT Services Management Support

The Contractor shall be responsible for recommending and supporting the development of IT service management plans, practices, infrastructures and systems utilizing industry best practices such as Information Technology Infrastructure Library (ITIL) to minimize negative impact on the IT enterprise. IT services management includes, but is not limited to:

A. Change Management
B. Release Management
C. Configuration Management
D. Incident Management
E. Problem Management
F. Service Desk Management
G. Availability Management
H. Capacity Management
I. Event Management
J. Data & Storage Management
K. Service Level Agreements (SLA)

4.1.9 Development Toolkits

The Contractor shall be responsible for recommending and supporting the utilization of development toolkits (e.g. IBM Rational ClearCase).

4.2 SYSTEMS/SOFTWARE ENGINEERING

The Contractor shall provide engineering expertise to analyze system concept, system design and interoperability, and provide recommendations for optimization. The Contractor shall review and analyze development, production, and system support proposals. The Contractor shall conduct trade-off/best technical approach analyses including cost estimation and cost benefit (e.g. Return on Investment (ROI)), analysis of alternatives, engineering studies, develop System Engineering Plans (SEPs), design plans, and technical reports as specified in the individual task order.

The Contractor shall provide systems/software engineering support for any or all phases of the system/software lifecycle to include Acquisition Strategy, Requirements Development, Requirements Management, Use Case Development, Risk Management, Architecture Design, Performance Engineering, Capacity Planning, System/Software Development, Test and Evaluation, and Sustainment. Requirements Development associated with iterative methodologies may occur at any phase of the development lifecycle. Therefore, requirements definition shall be structured to meet the incremental delivery needs of a particular project or program.

During the lifecycle process, software engineering support includes, but is not limited to software system reliability assessments, participation on governance boards and IPTs. The Contractor shall ensure the dependencies, interoperability, availability, reliability, maintainability and performance of the system as a whole within government provided guidelines specified in the individual task order.

The Contractor shall provide Business Process Modeling (BPM) to include clinical and benefits workflows and Business Process Reengineering (BPR) support to system/software engineering efforts. This includes developing activity and process models for analysis of requirements and identification of improvement opportunities. BPM may be a requirement for some software development projects.

4.2.1 Design and Development

The Contractor shall provide services with respect to all aspects and life-cycle phases which includes, but are not limited to planning, programming, requirements analysis, design, coding and unit testing, system integration testing, implementation, maintenance and updating of systems, applications, and/or services. This includes, but is not limited to healthcare and benefits information processing, payroll processing, financial management systems, decision support systems, and workflow management systems. The Contractor shall be fully cognizant of the implications of the VA strategic plan.

4.2.2 Architecture Development

The Contractor may support the enhancement of Enterprise Architectures and associated Technical Reference Models, as well as the development of Business Line Architectures and Solution Architectures. The Contractor may be involved in enterprise architecture assessments as well as infrastructure assessments. The Contractor may support the development of strategies and governance processes for architectures.

The Contractor may:

A. Develop process and data models derived from the VA Strategic Plan.
B. Develop the architecture, common infrastructure and services needed to support systems development (e.g. VistA, SOA, Open Source products)
C. Use common infrastructure and services to minimize the effort required to deliver new functional capabilities at a lower cost
D. Retire older systems and build new systems that are scalable and extensible by building them based on reusable services on commodity IT products
E. Conduct audits/assessments of the architectures and/or infrastructure

4.2.3 IT Service Management Implementation

The Contractor shall implement IT service management plans, practices, infrastructures and systems utilizing industry best practices such as ITIL and to minimize negative impact on the IT enterprise. IT services management includes, but is not limited to:

A. Change Management
B. Release Management
C. Configuration Management

D. Incident Management
E. Problem Management
F. Service Desk Management
G. Availability Management
H. Capacity Management
I. Event Management
J. Data & Storage Management

4.2.4 Enterprise Application/Services

The Contractor shall perform requirements analysis, system analysis, development and implementation support for core functional business and support applications and services, process re-engineering and adaptation of IT solutions in support of environments internal and external to the organization. Application support may include, but not limited to advanced collaboration capabilities, workflow, business process modeling, business process modeling translation, system modeling and simulation, software development, executive dashboards, enterprise search and discovery, project management and scheduling tools and applications and advanced multi-media support for training and marketing requirements.

4.2.5 Cloud Computing

The Contractor may be required to create and implement a cloud computing solution. The Contractor may also be required to support an existing cloud computing environment. Cloud computing is a delivery model for IT services based on the Internet, typically involving the provision of dynamically scalable and often virtualized resources as a service over the Internet. Cloud computing delivers common business applications online which are accessed from a web browser, while the software and data are stored on servers. These applications are broadly divided into the following categories, but are not limited to Infrastructure as a Service (IaaS), Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), Managed Service Providers (MSP), Service Commerce, and Internet Integration.

4.2.6 Web Application Design and Development

The Contractor shall provide services for evaluation, planning, requirements analysis, design, coding and unit testing, system integration testing, implementation, deploying, providing service to, maintaining or updating a web-based application or web-enabling a current system.

4.2.7 Mobile Application Design and Development

The Contractor shall provide services for evaluation, planning, requirements analysis, design, coding and unit testing, system integration testing, implementation, deploying, providing service for distributing, maintaining or updating a mobile application.

4.2.8 Human-Computer Interaction

The Contractor shall provide services related to analysis, design, evaluation, implementation, and testing of interactive and wearable computing systems for human use to include, but is not limited to telehealth, natural language processing, and 508 compliance.

4.2.9 System/Software Integration

The Contractor shall provide systems/software integration support to include planning, updating architecture models, interoperability specifications and analysis, system interface specifications, service definitions, and segmented architecture for the transition, integration, and implementation of IT systems.

4.2.10 Modeling and Simulation

The Contractor shall provide the personnel, equipment, tools and facilities necessary to model, simulate, and/or analyze IT services, systems, networks and other infrastructure or IT components in operation in the computing environment or under development. The Contractor may be required to model, simulate, or predict performance based on variables such as network latency, end-user device performance, and system-component upgrades. Modeling and simulation support may also include creating prototype implementations or developing mathematical models, as well as biomedical modeling and simulation. The level and type of modeling and simulation support required will be specified in the individual task order.

4.2.11 Informatics Services

The Contractor shall provide the following informatics services to include, but is not limited to assisting in the evaluation, analysis and recommendation of potential improvements and technology insertions, particularly in the areas of e-business technologies and architectures, health sciences, benefits management, collaboration tools and software, exchanging information and integrating systems and using data and KM. The Contractor shall develop, recommend, and implement KM strategies, policies, procedures, and best practices. The Contractor shall analyze and estimate the impact, operational effect, and supportability that the new technology will have on the existing processes, lifecycle cost, schedule, tradeoffs, interoperability, performance, suitability and other salient characteristics. The Contractor shall design, develop, implement, and maintain information management structures, systems and applications. In addition, the Contractor shall analyze new requirements and existing systems to determine and identify separable functions that are common across systems and potentially can be accommodated by COTS software, or alternatively by custom developed software. The Contractor shall conduct software engineering assessments on business process support systems to provide evaluation of modifiability, portability, reusability, performance and other quality areas. The Contractor shall also develop guidelines to include system/software architecture, software development processes, management indicators/quality metrics, requirements specifications and documentation standards. Data architecture repository and data architecture services are also included.

4.2.12 Engineering and Technical Documentation

The Contractor shall prepare and/or revise/update Engineering, User and Technical Documentation, Reports, and Manuals for existing or newly developed projects, software applications or systems.

4.2.13 Current System and Data Migration

These systems are in various stages of the lifecycle from Concept Exploration through and including Production, Deployment and system decommissioning. The migration of current systems and corresponding data to a common and enforced architecture within the VA Network

is the goal. Software engineering, data management, and Database Architecture support is required from the Contractor in the areas of computer resource management, analysis of technical documentation, participation in technical reviews, evaluation of test plans, system and integration testing, applicability studies and analysis of common software, and in the decommissioning of current systems.

4.2.14 Development Toolkit Support

The Contractor shall provide services that may include, but are not limited to acquisition and installation, administration, and maintenance of development toolkits (e.g. IBM Rational ClearCase).

4.3 SOFTWARE TECHNOLOGY DEMONSTRATION AND TRANSITION

The Contractors shall provide demonstrations and transition support for advanced software technologies. This functional area involves evaluating existing and emerging software technology products against the needs of current system development and support efforts, demonstrating specific technologies in the context of supported systems, and transitioning effective technology solutions into use. Current technology areas of focus for VA include software architectures, databases, web-based applications, mobile applications, telehealth, enterprise solutions, wireless, and security. This mission is a critical aspect of VA's ability to improve and advance its software engineering capability.

4.4 TEST & EVALUATION (T&E)

The Contractor shall provide T&E support in all phases of the systems/software development life cycle, to include preparation of test plans and procedures, design tests cases, conduct tests, witness tests and provide technical support, coordinate test plans IAW appropriate regulations, and analyze/evaluate/document test results. The Contractor shall participate in technical analyses, code reviews and other reviews as required.

4.5 INDEPENDENT VERIFICATION AND VALIDATION (IV&V)

The Contractor shall provide an independent review of products developed by other entities. The Contractor shall review, evaluate, validate and verify processes, procedures and methodologies used in developing, testing, maintaining and securing third-party systems/software.

4.6 ENTERPRISE NETWORK

The Contractor shall provide systems/network administration and infrastructure support, as well as data, voice and video systems services to meet the organization requirements.

4.6.1 Systems/Network Administration

The Contractor shall provide comprehensive support for the establishment, operation, administration, maintenance, migration, monitoring, analysis, and retirement of information systems, storage systems, network systems and security systems in locations worldwide for IT equipment currently within, or under consideration for procurement by VA, or other agencies. This includes, but is not limited to systems that support end-to-end Fault, Configuration, Administration, Performance, and Security (FCAPS) aspects of managing a network.

4.6.2 Network and Telecommunications Infrastructures

The Contractor shall provide services related to designing, delivering, operating, monitoring, maintaining, transitioning and decommissioning solutions up to turn-key communications systems. This may include, but is not limited to planning networks, designing infrastructure, engineering, installing, testing, and maintaining these network infrastructures. This includes all types of voice, data, and video networks, including converged networks of all three, as well as cloud computing solutions. These capabilities may also be provided as a service, e.g. voice-as-a-service (VaaS) and may be provided from telecommunications carriers.

4.6.2.1 Data Communications Systems

The Contractor shall provide services related to designing, delivering, operating, monitoring, maintaining, transitioning and decommissioning solutions for both secure and non-secure data communications systems which may include but is not limited to network management equipment, Asynchronous Transfer Mode (ATM) equipment, Internet Protocol (IP) equipment, channel banks, high-to-low level multiplex equipment, switching systems, Private Branch Exchange (PBX) systems, computer telephony interfaces, Channel Service Units (CSU), Digital Service Units (DSU), wireless, encryption tools and interfaces, signal conversion and interface equipment. This also includes all systems residing on the customer premises, beyond the carrier demarcation point.

4.6.2.2 Voice Systems

The Contractor shall provide services related to designing, delivering, operating, monitoring, maintaining, transitioning and decommissioning solutions for both secure and non-secure voice systems. This includes both existing systems as well as new installations. The voice systems will vary in size, location, network configuration, and functionality. This may include, but is not limited to engineering, furnishing, installing, and maintaining of legacy Private Branch Exchange (PBX) systems, Hybrid Voice over Internet Protocol-Time Division Multiplex (VoIP-TDM) systems, VoIP Systems, Automatic Call Distribution (ACD) systems, Intelligent Call Routing Systems, Healthcare and benefits specific systems, call center specific systems, and Interactive Voice Response (IVR) Systems. This will include working with leased voice solutions from telecommunications carriers.

4.6.2.3 Video Systems

The Contractor shall provide services related to designing, delivering, operating, monitoring, maintaining, transitioning and decommissioning solutions for both secure and non-secure video systems which may include Closed Circuit Television (CCTV), Cable TV (CATV), Video Teleconference (VTC) and desktop Local Area Network (LAN) VTC systems and web-based collaboration tools. These video systems may include, but are not limited to cameras, recorders, multipoint bridges, Integrated Services Digital Network (ISDN) and dial up systems, amplifiers, microphones, compression equipment, equalizers, remote controls, special optical enhanced equipment and video interface equipment. Video distribution may be wireless or over fiber optics, coaxial cable or twisted pair copper cable. The Contractor shall provide technical support for web-based collaboration training and other solutions.

4.6.2.4 Local Area Network (LAN)/Wide Area Network (WAN) Systems

The Contractor shall provide services related to designing, delivering, operating, monitoring, maintaining, transitioning and decommissioning solutions for both secure and non-secure turn-key LAN and WAN systems and components.

These systems may include the components of the physical layer including, but not limited to, inside and outside cable plant, wireless LAN, and WAN components. In terms of equipment, this may include, but is not limited to routers, Ethernet switches, multiplexers – Synchronous optical networking (SONET), Dense Wavelength Division Multiplexing (DWDM), network test equipment and network management systems.

4.6.2.5 Software Defined Networks

The Contractor shall provide services related to software defined network solutions.

4.6.2.6 Other Transmission Systems

The Contractor shall provide services related to designing, delivering and maintaining solutions for both secure and non-secure transmission systems which may include, but are not limited to single and multi-mode fiber optics, fiber optic multiplexing equipment, wireless, Radio Frequency (RF), satellite communications, fiber-to-copper and copper links, repeaters, switching protection and encryption.

4.7 ENTERPRISE MANAGEMENT FRAMEWORK

The Contractor shall provide services in support of executing the EMF, to include, but not limited to:

A. Development of Open Database Connectivity (ODBC)/ Java Database Connectivity (JDBC) connectors from existing software tools (for example: solar winds, SMS) to a federated data repository
B. Performance, Functionality and Validation testing and documentation of technologies (for example: WAN optimization, thin computing, virtualization, de-duplication, Virtual Desktop Infrastructure (VDI))
C. Testing which may involve the comparison of multiple technology vendors in support of a specific technology direction
D. Evaluation of the emerging technologies that enable organizational efficiencies
E. Development of solution driven architecture
F. Analysis and review of proposed solutions (internal and external) for technical merit and compliance to Organizational Technical Standards and published Standards
G. Information regarding any/all systems operating in the VA computing environment for inclusion in the One-VA Systems Inventory.

4.8 OPERATIONS AND MAINTENANCE (O&M)

The Contractor shall operate, repair, and maintain systems, applications, and IT environments in support of applications and/or system components for various environments. Environments requiring O&M tasks may include pre-production, production, test, training, disaster recovery/fail over, or any other combination of IT accounts. O&M includes but is not limited to, preventive maintenance and scheduled maintenance, activities to retain or restore systems (such

as testing, measurements, replacements, and adjustments), and other routine work required to maintain and/or enhance IT systems. The Contractor may also be required to provide software, infrastructure, platform, telecommunications and storage as a service through a subscription or other means. The Contractor may also be required to recommend best practice for requirements analysis, planning, design, deployment and ongoing operations management and technical support. The Contractor shall also maintain a current and up-to-date library of all operational documentation, logs of operational events, maintenance of operational monitoring and management tools, operational scripts and operational procedures.

4.8.1 Systems/Network Administration

The Contractor shall support IT hardware, operating systems, installation of software, monitoring and adjusting system performance, application of patches, security updates and service packs, repairs and upgrades of IT hardware. The Contractor shall monitor system resources such as processor, memory and disk utilization using automated monitoring tools, Monitor system logs, create system backups, schedules and tape allocation, establish/maintain access authorizations, perform installations, upgrades or replacements as required. All default software passwords shall be changed prior to moving to a production environment.

4.8.2 Application Support

The Contractor shall provide code level support for applications, scripts, and middleware software, including code review, debugging and patching, as well as error correction, defect repair and training of applications. The Contractor shall configure and install upgrades/patches to provided software per maintenance agreements using change and release management.

4.8.3 Hardware Support

The Contractor shall install, configure, patch, repair, upgrade, or remove hardware systems, components and operating systems. All default hardware passwords shall be changed prior to moving to a production environment.

4.8.4 Security Management

The Contractor shall provide services for A&A, IT security awareness, information protection awareness, organizationally mandated audit preparation, security test and evaluations, security incident management, and vulnerability analysis and testing.

4.8.5 Disaster Recovery (DR) and Continuity of Operations (COOP)

The Contractor shall provide services related to any and all methodologies pertaining to disaster recovery and business continuity. The range of recovery services under this functional area covers the spectrum from partial loss of function or data for a brief amount of time to a “worst-case” scenario in which a man-made, natural disaster, or IT failure results in the loss of the entire IT enterprise. Services may be required during any timeframe from initial declaration of a disaster to final recovery of all business processes.

4.8.6 Capacity/Availability Planning and Management

The Contractor shall perform services and analysis to ensure that IT capacity meets current and future business requirements in a cost-effective manner, based on historical utilization patterns and volume and forecast based on emerging requirements. The Contractor shall monitor

availability and maintenance requirements to sustain IT service-availability to support business in a cost-effective manner.

4.8.7 Service/Help Desk/Call Center Support

The Contractor shall deliver the full array of services, staff, and expertise to operate and maintain Service Desk/Help Desk/ Call Center functions as specified in individual Task Orders. The Contractor shall be required to participate in/support various aspects of applicable Service Operation processes (e.g., Incident Management, Event Management, Request Fulfillment, Access Management, Problem Management, etc.) as prescribed by the Task Order. The Contractor shall perform in a manner that is consistent with industry standard and best practice guidelines, while operating within the IT Service Management (ITSM) frameworks adopted and governed by organization policies, procedures and practices. Service-level requirements, metrics and other specifics shall be defined in each Task Order. Provide software system administration and operational support onsite or remotely as required. Install new software releases to supported locations/facilities/sites as required. This may include, but is not limited to individual computer and peripheral maintenance and desk side services.

4.8.8 Asset Management

The Contractor shall provide asset management support to include, but not limited to, inventory and utilization of software and hardware assets.

4.8.9 License Maintenance

The Contractor shall acquire, manage and maintain licenses and/or commercial maintenance agreements for use on all proprietary and commercial software as appropriate.

4.8.10 Database and Data Warehouse Administration

The Contractor shall provide services related to all types of data management, Database Management Systems (DBMS) and database applications including, but not limited to, logical and physical modeling and design/redesign, installation, administration, tailoring, tuning, troubleshooting, integrating, patching, upgrading, reporting, COOP, and backup/recovery/archiving/encryption and encryption key management. Development and maintenance, optimization, transition and decommissioning of Extract Transform Load (ETL) capabilities and scripts de-personalization of data, and data protection procedure development. The Contractor shall also provide data mining and Business Intelligence (BI) expertise to include, but is not limited to, product recommendation, selection, implementation, dashboard and report development, BI strategies, decision support, and data/report distribution. The Contractor shall also provide expertise to include enterprise capture, curation, storage, search, processing, sharing, transfer, analysis, virtualization, etc. This includes near real-time analytics including unstructured and structured, large and complex data on an enterprise scale. The Contractor may also be required to meet broad-based interoperability requirements at the Federal, state and local level.

4.8.11 Data Center Administration

The Contractor shall provide operations for the administration of Data Centers to include preventive maintenance, emergency services, and corrective services. Services may include the following: preventive maintenance schedules, coordination and tracking of service visits,

physical site inspections, invoice reviews for services, review of service reports, and resolution of service issues.

Physical operations and maintenance may include data center cleaning, Uninterruptible Power Supply (UPS) and battery maintenance, freestanding and rack-based power distribution of equipment, power and data cable physical inspections and corrections, generator and automatic transfer switch equipment, fire suppression and detection equipment, air-conditioning equipment, building Heating, Ventilation, and Air Conditioning (HVAC) and other physical facility maintenance tasks.

Data Center Administration may also include data center planning and design, power and cooling analysis, feasibility studies, risk assessments, site selection, energy usage assessments, virtualization strategies, optimization evaluations, and business continuity and disaster recovery, relocation or consolidation and IT technology roadmap planning.

The Contractor shall provide services related to software defined data center that includes a topology that extracts, pools and automates computations, networks and storage over multiple data centers including those owned by enterprises and service providers.

4.9 CYBER SECURITY

The Contractor shall define and deliver strategic, operational and process aspects of cyber security solutions. The Contractor shall ensure adequate LAN/Internet, data, information, and system security IAW organization standard operating procedures, conditions, laws, and regulations. The Contractor shall follow all applicable organization policies and procedures governing information security. VA mandates compliance with the protection of Personal Identification Information (PII).

4.9.1 Information Assurance (IA)

The Contractor shall identify, mitigate and resolve IA issues and concerns. The Contractor shall develop/contribute to guidelines/plans/policies, analyses and reviews that require IA expertise in the areas of assessments, monitoring, maintaining, reviewing and processing, A&A, accreditation/certification, Program Protection Plan (PPP) evaluation, and other cyber security related activities and mandates.

4.9.2 Logical Security

The Contractor shall establish, using National Institute Standards and Technology (NIST) Special Publications as a guide, secure logical and physical infrastructures for Information Systems (IS) environments including, but not limited to, security plans, risk assessments, access controls, directory services, compliance monitoring, firewalls, intrusion detection/scanning systems, anti-virus tools, privacy data assessment, and PII and other data protection policies. This function includes providing details for security awareness training, personnel security, policy enforcement, incident handling procedures, and separation of duties within an organization. In addition, the Contractor shall recommend and implement current best practices for the widest range of operating systems, database, networks, and application security, taking current best practices, industry standards, and Government regulations and policies into account.

4.9.3 Assessment and Authorization

The Contractor shall obtain commercial and/or organization specific certifications/authorizations for new or modified systems, applications, designs, equipment or installations IAW applicable organization standards specified by individual Task Orders. Specific activities include, but are not limited to security certifications, or comprehensive assessments of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly.

4.9.4 Security Operating Support

The Contractor shall provide operations support for Security Services including, but not limited to, Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS), Network Discovery, Security Device Monitoring, Compliance Scanning, Vulnerability Scanning Service (VSS), Vulnerability Management assistance, Patch Management, Anti-Virus Management Service (AVMS), Incident Response capabilities, Digital Forensics, Computer Network Defense, and Managed E-Authentication Service (MEAS). The operation support shall include, but is not limited to Managed Firewall Service (MFS), Web Content filtering monitoring, Virtual Private Network (VPN) or secure remote access maintenance and monitoring, and Web Application Firewalls. The Contractor shall provide services on a local or enterprise level. The Contractor shall also participate in security functions required to ensure the integrity and availability of computer systems including, but not limited to, security safeguard reviews, audits, reporting suspected security violations, acting to secure system environments, monitoring and responding to computer security alerts. Security Operating Support shall also include enterprise wide analysis of security based architecture, i.e., placement of Network Intrusion Prevention System (NIPS) devices, Centralized log management solutions, and data correlation activities.

4.10 TRAINING

The Contractor shall identify training requirements, obtain or develop training programs and conduct training for technologies, systems, applications and products at any stage of the lifecycle. This includes, but is not limited to IT workforce development and competency-based training, newly developed systems, as well as existing deployed systems, current systems, and any updates or changes to migrated systems. The Contractor shall develop training plans, manuals and other training documentation or training aids. Electronic training tools such as video teleconferencing and computer-based training shall be employed to enhance the effectiveness of training materials and courses. The Contractor shall conduct training for personnel to ensure proper operation, maintenance and testing of systems, applications and products. The Contractor shall provide training and knowledge transfer to technicians and other staff with regard to services and associated products delivered under any functional areas described herein. The training allows personnel the ability to operate and maintain the product or process in the future. The Contractor shall identify and/or provide any additional training required by end-users, technicians, or any other staff for implementation, maintenance and use of deliverables specified in individual Task Orders.

4.11 INFORMATION TECHNOLOGY FACILITIES

The Contractor shall provide a total IT solution to the client to include incidental facility design and modification services, conducting site surveys, facility connectivity, and installation.

4.11.1 Incidental Facility Design and Modification Services

The Contractor shall provide infrastructure design, installation, and modification services to support the IT solution. These activities may include, but are not limited to the modification of rooms or buildings at existing sites to support the information transport infrastructure required by the IT solution, furnishing and installing Category 5 or greater Unshielded Twisted Pair (UTP) and single or multimode fiber optic cabling, telecommunications pathways and spaces, work area outlet terminations, patch panels, racks, cabinets, fire-stop, fire suppression, telecommunications grounding and bonding, designing and installing fire-suppression systems. Affected rooms or buildings will be intended to host IT systems and provide work areas for the personnel operating them. Required activities may also include the dismantling and removal of the existing infrastructure in order to provide the modification services. This work shall be coordinated with the appropriate organization prior to the issuance of the work order. The work and the project approval documents must be executed by the appropriate installation engineering office and executed within the parameters of those approvals. The review may include, but is not limited to, master plan/land use plan compliance, utility systems capacity, and/or environmental constraints. Associated activities will be limited to incidental facility modification related to the project and would involve minimal real property maintenance, repair or modification activities.

4.11.2 Site Surveys

The Contractor shall perform the site surveys necessary to develop comprehensive plans for the installation of information transport systems and IT work areas. The survey shall provide input to Fixed Station Configuration Management Plans to include equipment reconfiguration requirements. This effort shall include, but is not limited to fully developed and dimensioned floor plan layouts, bills-of-material, telecommunications pathways and spaces, COOP/DR, telecommunications cabling, power distribution, environmental conditioning, test and cutover plans, grounding, access floor systems, lighting, backboards, labor estimations, required Government Furnished Equipment (GFE) and materials.

4.11.3 Facility Connectivity

The Contractor shall provide expertise in the design and installation of IT distribution systems which may include, but are not limited to, any and all approved inside plant fiber and copper media, media connectors, patch panels, fiber distribution cabinets, patch cords, pre-terminated cable assemblies, entrance facilities, first level backbone, second level backbone, horizontal distribution, termination blocks, wireless network components, cross-connects, and inter-connects. Knowledge of outside plant and aerial distribution methods may be required.

4.11.4 Installation

The Contractor shall install hardware and software/firmware as specified by individual Task Orders. Installation may involve fabrication of mounts, brackets and/or installation kits to include cabling, connections, and interconnecting devices. The Contractor shall assist the Government in identifying all equipment and utilities required for installation at the installation site, including Government Furnished Equipment/Material. The Government, with Contractor assistance, shall ensure that the required equipment, utilities, and resources are available at the installation site.

4.11.5 Physical Security Systems

The Contractor shall develop, implement and/or maintain the physical security functions to include building access guides, restricted access levels to facilities, biometrics or alarm systems.

5.0 DELIVERABLES

5.1 PRODUCTS

All products shall be delivered to the Government locations and accepted by authorized Government personnel as specified in the individual Task Order. Inspection and acceptance criteria shall be specifically identified in each Task Order. The COR shall be notified of any discrepancies found during acceptance inspection upon identification.

5.2 DATA

The Government shall receive Unlimited Rights to intellectual property first produced and delivered in the performance of this contract IAW FAR 52.227-14, Rights In Data-General (DEC 2007). This includes all rights to source code and any and all documentation created in support thereof. License rights in any Commercial Computer Software shall be governed by FAR 52.227-19, Commercial Computer Software License (DEC 2007). Any data delivered shall be submitted and protected IAW VA handbook 6500.

6.0 SECURITY AND PRIVACY

6.1 INFORMATION SECURITY AND PRIVACY SECURITY REQUIREMENTS

The Contractor shall comply with the VA security requirements IAW VA Handbook 6500.6 "Contract Security" and Addendum A of this document. VA Handbook 6500.6 Appendix C "VA Information Systems Security/Privacy Language for Inclusion into Contracts, As Appropriate" is included within this document as Addendum B. Addendum B may be tailored at the Task Order level.

6.2 PERSONNEL SECURITY REQUIREMENTS

The Contractor(s) shall comply with all personnel security requirements included in this contract and any unique organization security requirements described in each Task Order. All Contractor personnel who require access to VA sensitive information/computer systems shall be subject to background investigations and must receive a favorable background investigation from VA.

The position sensitivity risk designation [LOW/Tier 1, MODERATE/Tier 2, HIGH/Tier 4] and level of background investigation [National organization Check with Written Inquiries (NACI/Tier 1), Moderate Background Investigation (MBI/Tier 2), and/or Background Investigation (BI/Tier 4)] for each Task Order PWS task shall be designated accordingly, as identified within Section 4.6 of the TO PWS. The level and process of background security investigations for Contractors must be IAW VA Directive and Handbook 0710, "Personnel Suitability and Security Program".

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.

The Contractor shall bear the expense of obtaining background investigations.

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 ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (Refer to Section 4.6 of the Task Order PWS for investigative requirements by task), 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 one 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.

The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.

a. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints

The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify COR within 3 business days that documents were signed via eQIP).

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.

If the background investigation determination is not completed prior to the start date of work identified in each Task Order, 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) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).

The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.

Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.

Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

For DoD efforts, additional security clearance requirements will be identified at the TO order level.

6.3 FACILITY/RESOURCE PROVISIONS

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test

accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A Additional VA Requirements, Consolidated and ADDENDUM B - VA Information And Information System Security/Privacy Language.

6.4 BADGES

Employees working at a Government facility may be required to display, on their person, a Government-provided identification badge, that shall include the full name of the employee and the legal name under which the Contractor is operating. It is the responsibility of the Contractor to request and obtain badges from the Government prior to the first workday of any Contractor employee. The Contractor shall return all badges to the COR, or designee, on the same day an individual's employment is terminated and upon termination of the contract. The Contractor shall notify the Government program manager, or designee, immediately of any lost badges.

6.5 CLASSIFIED WORK

Work acquired on this contract for the Department of Defense or other Federal Agencies may involve secure networks, facilities and sensitive information. Specific security requirements and a suitability determination will be identified in the individual Task Order. The Contractor should anticipate potentially providing personnel with the security clearances up to the Top Secret level or Position Sensitivity of High/Tier 4 as required by the Task Order. Contractors must have the appropriate clearances for proposal purposes at the Task Order level.

6.6 INCIDENT REPORTING AND MANAGEMENT

The Contractor shall inform the COR, VA PM and assigned local Information Security Officer (ISO) of any security events and the Privacy Officer (PO) for any privacy violations within one hour of occurrence. Contractor will provide updates on the reported security/privacy events until closed by the ISO/PO.

6.7 SECURITY AND PRIVACY AWARENESS TRAINING

The Contractor shall complete the initial security and privacy awareness training and accept the VA Contractor Rules of Behavior (ROB) within three days of receipt of task order award in the VA Talent Management System (TMS). The Contractor shall complete the annual security and privacy awareness training and accept the VA Contractor ROB prior to expiration in the VA TMS.

6.8 SECURITY ROLE BASED TRAINING

The Contractor shall complete the assigned security role based training within three days in the TMS, upon assignment by the COR, as a prerequisite to receiving elevated privileges.

7.0 CONTRACT MANAGEMENT

7.1 GOVERNMENT SUPPORT

7.1.1 Task Order COR

A COR shall be designated for each Task Order. The COR shall be appointed by the CO and duties delegated in an appointment letter. The COR is the Requiring Activity's designated representative. The COR designated for each Task Order shall provide the Contractor access to all available Government furnished information, facilities, material, equipment, services as required to accomplish each Task Order. Contract surveillance duties shall be defined and accomplished IAW the Task Order Quality Assurance Surveillance Plan.

7.2 CONTRACTOR PROGRAM MANAGEMENT

The Contractor shall establish a single management focal point, the Program Manager, to accomplish the administrative, managerial and financial aspects of this contract and all subsequent Task Orders. This individual shall be identified to the TAC as the focal point for all programmatic issues.

7.2.1 Work Control

All program requirements, contract actions and data interchange shall be conducted in a digital environment using electronic and web-based applications. At minimum, such data shall be compatible with the Microsoft Office 2010® family of products, Microsoft Windows 7 products, Adobe Portable Document Format (PDF) and AutoCAD. The Government shall designate a standard naming convention for all electronic submissions within 60 days after contract award. The VA Acquisition Task Order Management System (ATOMS) portal shall be utilized for the interchange of data/documents (to include deliverables and invoices).

7.3 PRE-AWARD PROCEDURES

7.3.1 Request for Task Execution Plan (RTEP) Process

Upon identification of the need for a Task Order, a tracking number shall be assigned and the CO shall issue a RTEP to the Contractor. For Performance-Based tasks, the Government will specify requirements in terms of performance objectives. The Contractor shall propose "how to" best satisfy those objectives including proposed metrics to measure and evaluate performance.

7.3.1.1 Yes/No Bids

The Contractor shall post an electronic yes/no bid within two (2) working days after receipt of the RTEP on the Virtual Office of Acquisition (VOA) ATOMS module or as otherwise specified by the CO.

7.3.2 Task Execution Plan (TEP)

In order to meet contracting goals, the Government reserves the right to set-aside at the task order level. Otherwise, fair opportunity requirements shall be IAW applicable statutes, regulations, and case law. The Government's RTEP does NOT constitute an authorization to start work.

Within seven (7) work days of receipt of the RTEP, or unless otherwise specified in the RTEP, the Contractor shall submit one TEP IAW the format provided below unless otherwise specified by the CO. The following information shall be provided and submitted into the ATOMS portal:

A In addition to the information requested in the RTEP, the following shall be addressed in every TEP:

1. Proposal Summary Volume including:
    a. Task number
    b. Date submitted
    c. Contractor's name, Data Universal Numbering System (DUNS) and Commercial and Government Entity (CAGE) Code
    d. Contractor task leader contact information for questions
    e. Subcontractor(s) shall be identified by name, DUNS and CAGE Code at all tiers (as applicable)
    f. Proposed start and finish dates
    g. Proposed total price/cost
    h. Offerors are hereby advised that any Offeror-imposed terms and conditions which deviate from the Government's material terms and conditions established by the RTEP, may render the Offeror's proposal Unacceptable, and thus ineligible for award.
    i. If applicable, FAR 52.244-2 Subcontracts shall be addressed
    j. If the prime subcontracts 70% or greater, the prime shall provide a value-added statement for the proposed prime dollars IAW FAR 52.215-23 (Only applies to T&M and CR tasks)
    k. Duration for which proposal is valid (minimum 90 days)
    l. VAAR 852.209-70 is in effect for all RTEPs issued and the contractor should provide a statement IAW VAAR 852.209-70(b), when applicable
    m. Acknowledgement of Amendments.
    n. Contractors will be responsible for identifying any personnel subject to the SCA, and their corresponding region (state/county), within their proposed Task Execution Plans.

B The following shall be addressed only for T&M tasks:

1 A cost proposal volume shall be submitted in Microsoft Excel spreadsheet format. The first tab shall be a summary to include a top level rollup of the total dollars and percentages by labor, materials, travel, Other Direct Costs (ODC), and total Task Order cost. Labor shall further be broken out by labor category and hours. A separate tab shall be used for the Prime and each Subcontractor.

2 If you intend to propose subcontractor services in your TEP, provide a breakout of their costs for labor and material to include labor categories and an estimate of types and quantities of material, as well as, subcontract type (i.e. FFP, T&M or Cost). Subcontractors shall be identified at all tiers. The Government reserves the right to specify separate rates for each category of labor to be performed by each subcontractor and for each category of labor to be performed by the prime contractor, and for each

category of labor to be transferred between divisions, subsidiaries, or affiliates of the offeror under a common control.

3 The Labor Categories submitted shall reference the Government designated numbering scheme in the Labor Category Description Attachment 002.

4 When both the Prime and/or Subcontractor bid the Program Manager and/or Project Director, labor categories, detailed rationale shall be provided.

5 Material costs shall indicate raw material costs and material handling charges, as applicable. The nature and cost associated with each ODC shall be described

6 Bill of materials, indicating the source, quantity, unit cost and total cost for all required materials.

7 The Contractor shall notify the Government when using Department of Labor (DoL) labor categories. The notice shall provide what county and state the work is being performed in, and what labor categories are bid

8 The Contractor shall submit a completed Section B including all line items for base period and any options.

9 Offerors are hereby advised that any Pricing Assumptions which deviate from the Government's requirements or material terms and conditions established by the RTEP, may render the Offeror's proposal Unacceptable, and thus ineligible for award.

10 The Contractor shall address the adequacy of its accounting system as part of its price proposal.

C The following shall be addressed only for FFP tasks:

1 A price proposal volume shall be submitted in Microsoft Excel spreadsheet format. The first tab shall be a summary to include a top level rollup of the total dollars and percentages by labor, materials, travel, ODCs, and total Task Order price. Labor shall further be broken out by labor categories, labor rates, and hours. A separate tab shall be used for the Prime and each Subcontractor.

2 The Contractor shall submit a completed Section B including all priced line items for base period and any options.

3 Offerors are hereby advised that any Pricing Assumptions which deviate from the Government's requirements or material terms and conditions established by the RTEP, may render the Offeror's proposal Unacceptable, and thus ineligible for award.

4 "Information Other than Cost or Pricing Data" may be required where there is not "adequate price competition" as defined in FAR 15.403-1(c).

D The following shall be addressed only for CR tasks:

1 A cost proposal shall be submitted in Microsoft Excel spreadsheet format. The first tab shall be a summary to include a top level rollup of the total dollars and percentages by labor category, skill level, hours, materials, ODCs, and total Task Order cost. A separate tab shall be used for the Prime and each Subcontractor. When both the Prime and/or Subcontractor bid the Program Manager and/or Project Director, labor categories, detailed rationale shall be provided. Refer to the format set forth in FAR 15.408, Table 15-2, II and III as a guide.

2 If you intend to propose subcontractor services in your TEP, please provide a breakout of their costs for labor and material to include labor categories and an estimate of types and quantities of material, as well as, subcontract type (i.e. FFP, T&M or Cost). Subcontractors shall be identified at all tiers.
3 The Labor Categories submitted shall reference the Government designated numbering scheme in the Labor Category Description Attachment 002
4 Material costs shall indicate raw material costs and material handling charges, as applicable. The nature and cost associated with each ODC shall be described.
5 Bill of materials, indicating the source, quantity, unit cost and total cost for all required materials.
6 The Contractor shall notify the Government when using DoL labor categories. The notice shall provide the county and state the work is being performed in, and what labor categories are bid.
7 "Cost or Pricing Data" or "Information Other Than Cost or Pricing Data" may be required where there is not "adequate price competition" as defined in FAR 15.403-1
8 The Contractor shall submit a completed Section B including all line items for the base period and any option periods.
9 Offerors are hereby advised that any Pricing Assumptions which deviate from the Government's requirements or material terms and conditions established by the RTEP, may render the Offeror's proposal Unacceptable, and thus ineligible for award.
10 The Contractor shall address the adequacy of its accounting system as part of its price proposal.

E The following pertains to the preparation and submission of all TEPs:

1 Contractors are NOT to submit past performance as a part of their TEP, unless specified in the RTEP.
2 TEP Format
   a Proposal Summary
      i. Microsoft Word or PDF format
   b Technical Volume
      i Microsoft Word or PDF format
      ii No marketing materials; information relevant to the requirement only
   c Cost
      i. Shall be provided in Microsoft Excel
      ii. (T&M only) All Prime and Subcontractor Labor costs, Material costs, Travel, and ODCs must be broken out
         (a) (MS Excel) Summary Tab for Cost roll-up, and separate Tabs for Base Period and any Option
         (b) Separate tabs for Subcontractor(s)
         (c) Contractor shall notify the Government when using DOL labor categories. The notice shall provide in what County and State the work shall be performed, and what labor category(s) are bid
      iii. (Sole Source Cost and Firm, Fixed-price requirements) All Prime and Subcontractor Labor costs, Material costs, travel, and ODCs must be broken out per c. i and c. ii above

(a) Profit or fee identified as applicable
(b) "Information other than cost or pricing data" may be required where there is not "adequate price competition" as defined in FAR 15.403-1(c).

3 Page Limitations. When page limitations are specified in the RTEP, the following format shall apply:

The Summary and Technical Volumes will be submitted as an Acrobat PDF file or MS Word document. Price/Cost Volume shall be submitted in Microsoft Excel. Page size shall be no greater than 8 1/2" x 11". The top, bottom, left and right margins shall be a minimum of one inch each. Font size shall be no smaller than 12-point. 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 (minimum 6 point 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. 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. 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. Cover letter and Table of Contents are not included in the page count however any additional matrices, appendices, or acronym lists, etc will count against page limitation.

7.3.3 TEP Evaluation

The goal is to evaluate TEP submittals within 12 work days of receipt. Questions and clarifications may be required which can prolong the evaluation period. When requested by the CO, the Contractor shall provide a revised TEP to address changes.

All TEPs shall be subject to evaluation by a team of Government personnel. The evaluation team may also utilize non-Government advisors from Mitre Corporation to assist in the evaluation. The non-Government advisors will be required to sign Source Selection Participation Agreements which address conflicts of interest, rules of non-disclosure and rules of conduct. The chairperson of the Source Selection Evaluation Board (SSEB) will monitor the non-Government advisors' activities while in the evaluation area. This support will be limited to evaluation of the technical factor and only in those areas where Government expertise is not available. After the non-Government advisors have completed their particular area of evaluation, they will be released from the evaluation process. The non-Government advisors will only have access to the information corresponding to their area(s) of expertise. The company identified herein has agreed to abide by FAR Subpart 9.5, "Organizational Conflicts of Interest," and to refrain from disclosing proprietary information to unauthorized personnel. Reviews and approvals IAW FAR Part 35 and Part 37 have been obtained and documented.

7.4 ISSUANCE OF TASK ORDERS

Upon Government approval of the TEP and designation of an appropriate fund cite, the CO shall issue a Task Order to the Contractor. Contractor work shall commence only after issuance of the Task Order by the CO. The Government shall provide notification of task order award to both the successful and unsuccessful offerors.

7.5 LOGICAL FOLLOW-ONS

A logical follow-on may be issued IAW FAR 16.505 for services and/or products. A logical follow-on for maintenance/unique products shall only be authorized for economy and efficiency purposes as long as the services are on an existing or prior Task Order.

8.0 REPORTING AND MEETING REQUIREMENTS

8.1 REPORTING REQUIREMENTS

The deliverables defined below are required for the basic contract and each Task Order and shall be forwarded electronically to ATOMS (with the exception of the Contractor Staff Roster). The basic contract report shall be a rollup of each Task Order. Each individual Task Order report shall be delivered to the COR for that Task Order. Any differences between the requirements for the overall basic contract report versus the task order report are noted below. Each deliverable shall be submitted on a monthly basis (with the exception of the Contractor Staff Roster, Section 8.1.5) and shall be Section 508 compliant (for additional information concerning 508 Compliance see Addendum A3.0 and http://www.section508.va.gov/support/index.asp). Deliverables below will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance. The reporting period shall be from the first day of each month (or the date of Task Order award) through the last day of that month; each deliverable for that period shall then be submitted by the 15th day of each the following months.

8.1.1 Contractor's Progress, Status and Management Report

The Contractor shall submit a monthly Status Report. This report shall convey the status of all Task Orders awarded as of contract inception as well as cumulative contract performance. All relevant billing information shall be posted to the ATOMS portal. Task Orders that are completed shall be listed as such. A standard format is set forth in Section J Attachment 003, and shall be utilized for submission of the below required information. This report is required at the basic contract and shall be a rollup/summary of each task order. The task order report shall be unique to that task order only.

A For Each Task Order, indicate/discuss:

1. Task Order summary
2. Performance metrics
3. Task Order schedule
4. PMAS Compliancy (as applicable)
5. Critical items for Government review
6. Accomplishments

7. An itemized listing of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status
8. Significant open issues, risk and mitigation action
9. Summary of issues closed
10. Meetings completed
11. Projected meetings
12. Subcontractor performance – discuss 1st tier Subcontractor(s) performance
13. Projected activities for next reporting period
14. Explanation if the reporting period is over one month

B For Each Time and Materials Task, indicate:
1. High level summary
2. Expenditures for the reporting period
3. SLIN expenditure
4. Burn rate
5. Percentage of work completed
6. Set-Aside expenditures as applicable

C For Each Fixed Price Task indicate:
1. Invoice/receiving report submitted
2. Milestone payment schedule
3. Set-Aside Expenditures as applicable

D For Each Cost Task, indicate:
1. High level summary
2. Expenditures for the reporting period
3. SLIN expenditure
4. Burn rate
5. Percentage of work completed
6. Set-Aside Expenditures as applicable

E General and Cumulative Performance. Indicate the following:
1 Any general meetings that occurred with Government representatives during the reporting period
2 Total dollars awarded to date (ceiling)
3 Total dollars invoiced to date, by fiscal year, and since contract award. These figures shall be further broken out by dollars and percentage of time and materials invoices vs. fixed price invoices.

8.1.2 Contract Performance Report (CPR)

This report is required at the basic contract and shall be a rollup/summary of each task Order. The overall basic contract report shall show the detail for each Task Order with a summary column for the entire program. The Task Order report shall be unique to that Task Order only. This report is not required for Firm Fixed Price Task Orders. Contractors may be required to support EVMS (Earned Value Management System) at the Task Order level.

A For Each Time and Materials Task, indicate:
   1 Expenditures for the reporting period by labor, material and ODCs
   2 Labor costs shall be broken down by assigned numbering system for contract, Task Order and labor category, entity (Prime or Subcontractor), rates and hours
   3 Material costs and ODCs shall be identified by type, and subcontractor (as applicable), and discussed
   4 Total task expenditures for the fiscal year to date, indicated as total, labor, materials and ODCs
   5 Total task expenditures since task award, indicated as total, labor, materials and ODCs
   6 The Contract Performance Report as set forth in Section J, Attachment 004**,** shall be submitted monthly via the ATOMS portal.

B For Each Cost Task, indicate:
   1 Labor costs broken down by assigned numbering system for contract, Task Order and labor category, skill level, entity (Prime or Subcontractor) rate and hours, material costs, ODCs, Cost of Money and fee.
   2 Total task expenditures for the fiscal year to date, indicated as total labor, materials, ODCs, Cost of Money, and fee.
   3 Total task expenditures since task award, indicated as total, labor, materials, ODCs, Cost of Money, and fee.
   4 The Contract Performance Report as set forth in Section J, Attachment 005, shall be submitted monthly via the ATOMS portal.

8.1.3 Status of Government Furnished Equipment (GFE) Report

This report is required at the basic contract and shall be a rollup/summary of each task order. The overall basic contract report shall show the detail for each task order with a summary column for the entire program. The task order report shall be unique to that task order only.

A. Task Order
B. Project Name
C. Type of Equipment
D. Tracking Number
E. Location
F. Value
G. Total Number of Pieces
H. Total Value of Equipment
I. Anticipated Transfer Date to Government
J. Anticipated Transfer Location
K. The Government Furnished Equipment Report as set forth in Section J, Attachment 006, shall be submitted monthly via the ATOMS portal

8.1.4 Personnel Contractor Manpower Report

The Contractor shall provide a Personnel Report (MS Excel), on a monthly basis listing all personnel under each Task Order. As personnel changes occur, a revised report is required only for the individual Task Order affected for Background Investigations. The overall basic contract report should only be updated on the monthly basis. The overall basic contract report shall show

the detail for each task order with a summary column for the entire program. The individual task order report will be unique to that task order. The information required is as follows:

A. Task Order
B. OI&T Pillar Supported
C. Employee Name
D. Background Investigation/Clearance level and/or Status
E. Company name
F. Prime/Subcontractor
G. Labor Category
H. Facility location
I. Tour of Duty Schedules (e.g. Monday through Friday, 9:00 am to 5:00 pm)
J. Universal Unique Identifier UUID (Badge Number bottom right of back of badge)
K. Facility where badge was issued
L. Badge Expiration Date
M. Project supporting
N. Date Disassociated From Contract (for employees who no longer support this contract)
O. Date Badge Returned to COR
P. Contractor Rules of Behavior
Q. VA Cyber Security Awareness and Rules of Behavior Training
R. Annual VA Privacy Training
S. The Personnel Contractor Manpower Report as set forth in Section J, Attachment 007(basic) and 008 (task order), shall be submitted monthly via the ATOMS portal

8.1.5 Contractor Staff Roster

The Contractor shall provide a Task Order Contractor Staff Roster, in accordance with the ProPath template, of Contractor and Subcontractor employees within three business days after Task Order award for all personnel employed under each Task Order to begin their background investigations. As personnel changes occur a revised roster is required. The Contractor Staff Roster shall be updated and delivered only to the COR within one 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. Do not post the Contractor Staff Roster on ATOMS. The Contractor Staff Roster should indicate which employees are active or inactive. For inactive employees, the roster should indicate the date the employee was separated from the Task Order and their credentials returned to the COR.

The Contractor Staff Roster shall contain:

A. Contractor's Full Name
B. Email Address
C. Place of Birth
D. Date of Birth
E. Security/Privacy Training Completion Dates
F. Risk Designation-individual background investigation level requirement (Refer to Section 4.6 of the Task Order PWS for investigative requirements by task)
G. Existing Background Investigation and/or Clearance (if applicable)

H. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. 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.

8.1.6 Small Business Participation Report

The Contractor shall submit the Small Business Participation Report, on a quarterly basis.

The Small Business Participation Report shall contain:

A. Company Name
B. Company Cage Code/DUNS Number:
C. Company Size
D. T4NG Prime Contract Number
E. Date Report Submitted
F. POC for questions on this report (name, phone, email)
G. Small Business Particpation Quarter and Year
H. Total Obligated Dollars (cumulative to date)
I. Funded/Obligated Small Business Dollars and Total Obligated Dollars for Total Small Business Subcontracting Participation (Goal 1 Small Business Actuals)
J. Small Business Category Cumulative Funded/Obligated Dollars and Total Obligated Dollars for (GOAL 2 - Breakout of Small Business Dollars on Total Contract Obligated Dollars):
    1. Small Disadvantaged Business
    2. Women Owned Small Business
    3. HUBZone
    4. Veteran Owned Small Business
    5. Service Disabled Veteran Owned Small
    6. Small Business (No other category above)
K. Explanation (as necessary)
L. Subcontractor Identification
    1. Subcontractor Name
    2. Subcontractor Status
    3. Total Dollars Obligated (Cumulative)

8.1.7 Veterans Employment Certification Report

The Contractor shall provide a Veterans Employment Certification Report, on a quarterly basis listing the following:

A. Total number of employees at time of proposal submission
B. Total number of Veterans employed at time of proposal submission
C. Total number of current employees
D. Total number of current Veterans employed

The Contractor's Chief Executive Officer (CEO), or equivalent, shall certify in the Veterans Employment Certification Report that the that the Contractor has, in good faith, relied on the

representations of its employees to derive the total number of employees and the number of Veterans that it employs.

8.2 MEETINGS AND REVIEWS

For successful management and contract surveillance, the following meetings and reviews are required.

8.2.1 Project Office Initial Program Review (IPR)

The VA TAC shall host an IPR within 30 days after contract award to review the PWS, business policies, and procedures, and introduce personnel.

8.2.2 Post-Award Conferences

The Government intends to convene a Post-Award Conference with each awardee within 60 days after contract award. The CO shall notify all Prime Contractors of a specific date, location and agenda within 30 days after contract award.

8.2.3 Program Reviews

At the discretion of the CO, Program Review Meetings shall be conducted by the VA TAC Contract Specialist and/or designated COR for each contract. Dates, locations, agenda, and attendance requirements shall be specified by the appropriate Government representative, at least five (5) calendar days prior to the meeting.

8.2.4 Quarterly Collective Prime Program Reviews

The VA TAC shall host a quarterly Prime Program Review with the designated Prime Program Manager and one attendee. Dates, locations, and agenda shall be specified at least five (5) calendar days prior to the meeting.

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, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

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

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

A2.0 VA Enterprise Architecture Compliance

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

A2.1 VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's

Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

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

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

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

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

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards and http://www.section508.gov/content/learn/standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

Additional requirements may be specified at the Task Order Level.

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 Contracting Officer 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 Contracting Officer 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 Contracting Officer.
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.

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 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; 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. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

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

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

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

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

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

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B.1 GENERAL

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

B.2 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

c. Contract personnel who require access to national security programs must have a valid security clearance. 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 Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B.3 VA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in 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).

b. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's 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.

c. 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 Contracting Officer within 30 days of termination of the contract.

d. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST

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

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

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

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

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

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

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

k. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the

Contractor/Subcontractor 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 contracting officer for response.

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

B.4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. 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 Appendix D of VA Handbook 6500, *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, *VA Privacy Impact Assessment*.

b. 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 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

c. 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.

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

e. 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, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

f. 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.

g. The Contractor/Subcontractor agrees to:

1) 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:

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the Contractor/Subcontractor is to perform;

2) 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

3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

h. 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.

1) "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.

2) "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.

3) "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.

i. 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.

j. 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 _____days.

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

l. 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 contracting officer and the VA Assistant Secretary for Office of Information and Technology.

B.5 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's network involving VA information must be reviewed and approved by VA prior to implementation.

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

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

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

B.6 SECURITY INCIDENT INVESTIGATION

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

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

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

d. In instances of theft 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.

B.7 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.

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 Security and Privacy Incidents*, 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:

2) Notification;

3) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;

4) Data breach analysis;

5) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;

6) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

7) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B.8 SECURITY CONTROLS COMPLIANCE TESTING

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

B.9 TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

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

2) Successfully complete the appropriate VA Privacy training and annually complete required privacy training;

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 contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]*

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

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 H - SPECIAL CONTRACT REQUIREMENTS

H.9 METRICS

The T4NG contract is performance based and IAW FAR 37.102, task orders issued under T4NG will be performance-based to the maximum extent practicable. Contractor performance on the Task Order level will be assessed IAW the corresponding QASP Performance Based Service Assessment Survey. After 6-months of performance history under the program, past performance and past performance in achieving small business participation goals, may be added as possible evaluation criteria in task order competition as well as reviewing Contractor performance.

Task Order Metrics: (at a minimum)

1. Technical Quality of Product or Service : "3" or Above in each category
2. Project Milestones and Schedule: "3" or Above in each category
3. Cost and Staffing: "3" or Above in each category
4. Management: "3" or Above in each category

Task orders will include remedies and may include incentives tailored for individual task orders based on task order type and associated risks.

H-12NOTIFICATION OF SATISFACTION SURVEY: ACQUISITION 360 (JULY 2015)

b. This acquisition has been identified as being a complex information technology (IT) development, systems, or services. As a result, your company may receive a survey pursuant to the Office of Management and Budget's (OMB) memorandum dated March 18, 2015 entitled, Acquisition 360 – Improving the Acquisition Process through Timely Feedback from External and Internal Stakeholders. The survey will ask your company to rate various aspects of the acquisition process, such as the strength of the requirements development process, the clarity of the solicitation, and the effectiveness of the agency in executing awards and debriefing offerors. The overall goal of the survey is to help the agency identify strengths and weaknesses with industry partnerships so that it can make internal improvements on the planning and making of contract awards.

(b) The Federal Government may not conduct or sponsor, and the public is not required to respond to, a collection of information that does not display a currently valid OMB control number. The OMB control number for this collection is 1505-0231. If your company receives a survey, your company is strongly encouraged, but not required to respond. The survey should take no more than ten (10) minutes to complete. The results of the surveys will be submitted to the agency's senior procurement officials in order to identify best practices and areas in need of improvement, necessary to strengthen the agency's acquisition practices.

(c) Should you have any question regarding the survey process, contact the contracting officer responsible for the identified IT acquisition. (End of provision)

PART II - CONTRACT CLAUSES

SECTION I - CONTRACT CLAUSES

I.2 52.203-99, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements (DEVIATION 2015-02)

(a) The Contractor shall not require employees or contractors seeking to report fraud, waste, or abuse to sign or comply with 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.

(b) The contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this clause are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d)(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(2) The Government may seek any available remedies in the event the contractor fails to comply with the provisions of this clause.

(End of clause)

I.3 52.209-10 – Prohibition on Contracting With Inverted Domestic Corporations.

As prescribed in 9.108-5(b), insert the following clause:

Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015)

(a) Definitions. As used in this clause--

“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).

“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.

(b) If the contractor reorganizes as an inverted domestic corporation or becomes a subsidiary of an inverted domestic corporation at any time during the period of performance of this contract, the Government may be prohibited from paying for Contractor activities performed after the date when it becomes an inverted domestic corporation or subsidiary. The Government may seek any available remedies in the event the Contractor fails to perform in accordance with the terms and conditions of the contract as a result of Government action under this clause.

(c) Exceptions to this prohibition are located at 9.108-2.

(d) In the event the Contractor becomes either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation during contract performance, the Contractor shall give written notice to the Contracting Officer within five business days from the date of the inversion event.

(End of clause)

I.4 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the “maximum.” The Government shall order at least the quantity of supplies or services designated in the Schedule as the “minimum.”

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor’s and Government’s rights and obligations with respect to that order to the same extent as if the order were completed during the contract’s effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 60 months.

(End of clause)

I.5 52.222-55 MINIMUM WAGES UNDER EXECUTIVE ORDER 13658 (DEC 2014)

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

“United States" means the 50 states and the District of Columbia.

“Worker"—

(1) Means any person engaged in performing work on, or in connection with, a contract covered by Executive Order 13658, and—

(i) Whose wages under such contract are governed by the Fair Labor Standards Act (29 U.S.C. chapter 8), the Service Contract Labor Standards statute (41 U.S.C. chapter 67), or the Wage Rate Requirements (Construction) statute (40 U.S.C. chapter 31, subchapter IV);

(ii) Other than individuals employed in a bona fide executive, administrative, or professional capacity, as those terms are defined in 29 CFR part 541; and

(iii) Regardless of the contractual relationship alleged to exist between the individual and the employer.

(2) Includes workers performing on, or in connection with, the contract whose wages are calculated pursuant to special certificates issued under 29 U.S.C. 214(c).

(3) Also includes any person working on, or in connection with, the contract and individually registered in a bona fide apprenticeship or training program registered with the Department of Labor's Employment and Training Administration, Office of Apprenticeship, or with a State Apprenticeship Agency recognized by the Office of Apprenticeship.

(b) *Executive Order Minimum Wage rate.*

(1) The Contractor shall pay to workers, while performing in the United States, and performing on, or in connection with, this contract, a minimum hourly wage rate of $10.10 per hour beginning January 1, 2015.

(2) The Contractor shall adjust the minimum wage paid, if necessary, beginning January 1, 2016, and annually thereafter, to meet the applicable annual E.O. minimum wage. The Administrator of the Department of Labor's Wage and Hour Division (the Administrator) will publish annual determinations in the Federal Register no later than 90 days before the effective date of the new E.O. minimum wage rate. The Administrator will also publish the applicable E.O. minimum wage on www.wdol.gov (or any successor Web site) and a general notice on all wage determinations issued under the Service Contract

Labor Standards statute or the Wage Rate Requirements (Construction) statute, that will provide information on the E.O. minimum wage and how to obtain annual updates. The applicable published E.O. minimum wage is incorporated by reference into this contract.

(3)

(i) The Contractor may request a price adjustment only after the effective date of the new annual E.O. minimum wage determination. Prices will be adjusted only for increased labor costs (including subcontractor labor costs) as a result of an increase in the annual E.O. minimum wage, and for associated labor costs (including those for subcontractors). Associated labor costs shall include increases or decreases that result from changes in social security and unemployment taxes and workers' compensation insurance, but will not otherwise include any amount for general and administrative costs, overhead, or profit.

(ii) Subcontractors may be entitled to adjustments due to the new minimum wage, pursuant to paragraph (b)(2). Contractors shall consider any subcontractor requests for such price adjustment.

(iii) The Contracting Officer will not adjust the contract price under this clause for any costs other than those identified in paragraph (b)(3)(i) of this clause, and will not provide duplicate price adjustments with any price adjustment under clauses implementing the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute.

(4) The Contractor warrants that the prices in this contract do not include allowance for any contingency to cover increased costs for which adjustment is provided under this clause.

(5) A pay period under this clause may not be longer than semi-monthly, but may be shorter to comply with any applicable law or other requirement under this contract establishing a shorter pay period. Workers shall be paid no later than one pay period following the end of the regular pay period in which such wages were earned or accrued.

(6) The Contractor shall pay, unconditionally to each worker, all wages due free and clear without subsequent rebate or kickback. The Contractor may make deductions that reduce a worker's wages below the E.O. minimum wage rate only if done in accordance with 29 CFR 10.23, Deductions.

(7) The Contractor shall not discharge any part of its minimum wage obligation under this clause by furnishing fringe benefits or, with respect to workers whose wages are governed by the Service Contract Labor Standards statute, the cash equivalent thereof.

(8) Nothing in this clause shall excuse the Contractor from compliance with any applicable Federal or State prevailing wage law or any applicable law or municipal ordinance establishing a minimum wage higher than the E.O. minimum wage. However,

wage increases under such other laws or municipal ordinances are not subject to price adjustment under this subpart.

(9) The Contractor shall pay the E.O. minimum wage rate whenever it is higher than any applicable collective bargaining agreement(s) wage rate.

(10) The Contractor shall follow the policies and procedures in 29 CFR 10.24(b) and 10.28 for treatment of workers engaged in an occupation in which they customarily and regularly receive more than $30 a month in tips.

(c)

(1) This clause applies to workers as defined in paragraph (a). As provided in that definition--

(i) Workers are covered regardless of the contractual relationship alleged to exist between the contractor or subcontractor and the worker;

(ii) Workers with disabilities whose wages are calculated pursuant to special certificates issued under 29 U.S.C. 214(c) are covered; and

(iii) Workers who are registered in a bona fide apprenticeship program or training program registered with the Department of Labor's Employment and Training Administration, Office of Apprenticeship, or with a State Apprenticeship Agency recognized by the Office of Apprenticeship, are covered.

(2) This clause does not apply to--

(i) Fair Labor Standards Act (FLSA)-covered individuals performing in connection with contracts covered by the E.O., i.e. those individuals who perform duties necessary to the performance of the contract, but who are not directly engaged in performing the specific work called for by the contract, and who spend less than 20 percent of their hours worked in a particular workweek performing in connection with such contracts;

(ii) Individuals exempted from the minimum wage requirements of the FLSA under 29 U.S.C. 213(a) and 214(a) and (b), unless otherwise covered by the Service Contract Labor Standards statute, or the Wage Rate Requirements (Construction) statute. These individuals include but are not limited to--

(A) Learners, apprentices, or messengers whose wages are calculated pursuant to special certificates issued under 29 U.S.C. 214(a).

(B) Students whose wages are calculated pursuant to special certificates issued under 29 U.S.C. 214(b).

(C) Those employed in a bona fide executive, administrative, or professional capacity (29 U.S.C. 213(a)(1) and 29 CFR part 541).

(d) *Notice*. The Contractor shall notify all workers performing work on, or in connection with, this contract of the applicable E.O. minimum wage rate under this clause. With respect to workers covered by the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, the Contractor may meet this requirement by posting, in a prominent and accessible place at the worksite, the applicable wage determination under those statutes. With respect to workers whose wages are governed by the FLSA, the Contractor shall post notice, utilizing the poster provided by the Administrator, which can be obtained at www.dol.gov/whd/govcontracts, in a prominent and accessible place at the worksite. Contractors that customarily post notices to workers electronically may post the notice electronically provided the electronic posting is displayed prominently on any Web site that is maintained by the contractor, whether external or internal, and customarily used for notices to workers about terms and conditions of employment.

(e) *Payroll Records.*

(1) The Contractor shall make and maintain records, for three years after completion of the work, containing the following information for each worker:

(i) Name, address, and social security number;

(ii) The worker's occupation(s) or classification(s);

(iii) The rate or rates of wages paid;

(iv) The number of daily and weekly hours worked by each worker;

(v) Any deductions made; and

(vi) Total wages paid.

(2) The Contractor shall make records pursuant to paragraph (e)(1) of this clause available for inspection and transcription by authorized representatives of the Administrator. The Contractor shall also make such records available upon request of the Contracting Officer.

(3) The Contractor shall make a copy of the contract available, as applicable, for inspection or transcription by authorized representatives of the Administrator.

(4) Failure to comply with this paragraph (e) shall be a violation of 29 CFR 10.26 and this contract. Upon direction of the Administrator or upon the Contracting Officer's own action, payment shall be withheld until such time as the noncompliance is corrected.

(5) Nothing in this clause limits or otherwise modifies the Contractor's payroll and recordkeeping obligations, if any, under the Service Contract Labor Standards statute, the Wage Rate Requirements (Construction) statute, the Fair Labor Standards Act, or any other applicable law.

(f) *Access*. The Contractor shall permit authorized representatives of the Administrator to conduct investigations, including interviewing workers at the worksite during normal working hours.

(g) *Withholding*. The Contracting Officer, upon his or her own action or upon written request of the Administrator, will withhold funds or cause funds to be withheld, from the Contractor under this or any other Federal contract with the same Contractor, sufficient to pay workers the full amount of wages required by this clause.

(h) *Disputes*. Department of Labor has set forth in 29 CFR 10.51,Disputes concerning contractor compliance, the procedures for resolving disputes concerning a contractor's compliance with Department of Labor regulations at 29 CFR part 10. Such disputes shall be resolved in accordance with those procedures and not the Disputes clause of this contract. These disputes include disputes between the Contractor (or any of its subcontractors) and the contracting agency, the Department of Labor, or the workers or their representatives.

(i) *Antiretaliation*. The Contractor shall not discharge or in any other manner discriminate against any worker because such worker has filed any complaint or instituted or caused to be instituted any proceeding under or related to compliance with the E.O. or this clause, or has testified or is about to testify in any such proceeding.

(j) *Subcontractor compliance*. The Contractor is responsible for subcontractor compliance with the requirements of this clause and may be held liable for unpaid wages due subcontractor workers.

(k) *Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (k) in all subcontracts, regardless of dollar value, that are subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, and are to be performed in whole or in part in the United States.

(End of clause)

I.6 52.232-39 Unenforceability of Unauthorized Obligations (JUN 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement , that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(1) Any such clause is unenforceable against the Government.

(2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulation and procedures.

(End of clause)

PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

SECTION J - LIST OF ATTACHMENTS

Attachment 001 - Pricing Attachment

Attachment 002 - Labor Category Descriptions

Attachment 003 - Contractor's Progress Status and Management Report

Attachment 004 - Contract Performance Report for TM

Attachment 005 - Contract Performance Report for CF

Attachment 006 - Government Furnished Equipment (GFE) Report

Attachment 007 - Manpower Report - Basic

Attachment 008 - Manpower Report - Task Order

Attachment 009 - Contractor Staff Roster Template

Attachment 010 - Small Business Participation Report

Attachment 011 - Veterans Employment Certification Report

Attachment 012 - Price Methodology