5. PROJECT NO.

CODE

7. ADMINISTERED BY

2. AMENDMENT/MODIFICATION NO.

CODE

6. ISSUED BY

8. NAME AND ADDRESS OF CONTRACTOR

4. REQUISITION/PURCHASE REQ. NO.

3. EFFECTIVE DATE

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED

PAGE OF PAGES

10A. MODIFICATION OF CONTRACT/ORDER NO.

10B. DATED

BPA NO.

1. CONTRACT ID CODE

FACILITY CODE

CODE

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:

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers

E. IMPORTANT:

is extended,

(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 AC-

KNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY

is not extended.

12. ACCOUNTING AND APPROPRIATION DATA

(REV. 10-83)

is required to sign this document and return \_\_\_\_\_\_\_\_\_\_\_ copies to the issuing office.

is not,

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.

15C. DATE SIGNED

B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES

SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).

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.

C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:

D. OTHER

BY

Contractor

16C. DATE SIGNED

14. DESCRIPTION OF AMENDMENT/MODIFICATION

16B. UNITED STATES OF AMERICA

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

16A. NAME AND TITLE OF CONTRACTING OFFICER

15B. CONTRACTOR/OFFEROR

STANDARD FORM 30

NSN 7540-01-152-8070

PREVIOUS EDITION NOT USABLE

Prescribed by GSA - FAR (48 CFR) 53.243

(Type or print)

(Type or print)

(Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

(No., street, county, State and ZIP Code)

(If other than Item 6)

(Specify type of modification and authority)

(such as changes in paying office, appropriation date, etc.)

(If required)

(If applicable)

(SEE ITEM 11)

(SEE ITEM 13)

(X)

(X)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS,

IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

(Signature of person authorized to sign)

(Signature of Contracting Officer)

1

59

A00003

TAC-13-06567

Department of Veterans Affairs

Technology Acquisition Center

260 Industrial Way West

Eatontown NJ 07724

Department of Veterans Affairs

Technology Acquisition Center

260 Industrial Way West

Eatontown NJ 07724

To all Offerors/Bidders

VA118-13-R-0042

X

x

x

1

May 9, 2013 12:00PM EST

x

1

The purpose of this amendment is to initiate Step Two of the RFP, to provide a revised Performance Work Statement, and

to revise Section L.6 Proposal Submission instructions pertaining to price methodology file in Volume V - PRICE.

Eligible offerors are required to submit a response to Step Two by noon on May 9, 2013.

A revised Performance Work Statement dated January 11, 2013 is hereby provided and supersedes the previous version.

All other terms and conditions remain unchanged and in full force and effect.

# SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

**Performance Work Statement (PWS)**

**for the**

**Transformation Twenty-One Total Technology (T4)**

**Program**

**JANUARY 11, 2013**

**Department of Veterans Affairs**

**Office of Acquisition Operations (OAO)**

**Technology Acquisition Center (TAC)**

TABLE OF CONTENTS

[SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK 2](#_Toc352757715)

[1.0 SCOPE 6](#_Toc352757716)

[2.0 APPLICABLE DOCUMENTS 6](#_Toc352757717)

[3.0 GENERAL REQUIREMENTS 7](#_Toc352757718)

[3.1 Contract Type 7](#_Toc352757719)

[3.2 Period of Performance 8](#_Toc352757720)

[3.3 Place of Performance 8](#_Toc352757721)

[3.4 Travel 8](#_Toc352757722)

[3.5 Materials, Equipment and Facilities 8](#_Toc352757723)

[3.5.1 Government-Furnished 8](#_Toc352757724)

[3.5.2 Contractor-Acquired 8](#_Toc352757725)

[3.5.3 Non-Developmental Items and Commercial Processes 9](#_Toc352757726)

[3.5.4 Connectivity 9](#_Toc352757727)

[3.5.5 Facilities 9](#_Toc352757728)

[3.5.6 Warranty 9](#_Toc352757729)

[3.5.7 Marking, Handling, Storage, Preservation, Packaging, & Shipping 9](#_Toc352757730)

[3.5.8 Export Control 9](#_Toc352757731)

[3.7 Safety and Environmental 10](#_Toc352757732)

[3.8 Enterprise and IT Framework 10](#_Toc352757733)

[3.9 Commercial Development Methodologies 11](#_Toc352757734)

[3.10 Integrated Product Teams 11](#_Toc352757735)

[3.11 Quality Assurance 11](#_Toc352757736)

[3.12 Transition and Orientation Support 12](#_Toc352757737)

[4.0 TECHNICAL FUNCTIONAL AREAS 12](#_Toc352757738)

[4.1 Program Management, Strategy, Enterprise Architecture and Planning Support 12](#_Toc352757739)

[4.1.1 Strategy and Planning 12](#_Toc352757740)

[4.1.2 Standards, Policy, Procedure and Process Development, and Implementation Support 12](#_Toc352757741)

[4.1.3 Requirements Development and Analysis Support 13](#_Toc352757742)

[4.1.4 Technology Refresh and Configuration Reviews 13](#_Toc352757743)

[4.1.5 Studies and Analyses 13](#_Toc352757744)

[4.1.6 Program Management Support 14](#_Toc352757745)

[4.1.7 Product Data 14](#_Toc352757746)

[4.1.8 IT Services Management Guidance 14](#_Toc352757747)

[4.1.9 Development Toolkit Guidance 15](#_Toc352757748)

[4.2 Systems/Software Engineering 15](#_Toc352757749)

[4.2.1 Design and Development 15](#_Toc352757750)

[4.2.2 Architecture Development 16](#_Toc352757751)

[4.2.3 IT Service Management Implementation 16](#_Toc352757752)

[4.2.4 Enterprise Application/Services 16](#_Toc352757753)

[4.2.5 Web Application Design and Development 16](#_Toc352757754)

[4.2.6 Human-Computer Interaction 17](#_Toc352757755)

[4.2.7 System/Software Integration 17](#_Toc352757756)

[4.2.8 Modeling and Simulation 17](#_Toc352757757)

[4.2.9 Informatics Services 17](#_Toc352757758)

[4.2.10 Engineering and Technical Documentation 17](#_Toc352757759)

[4.2.11 Current System and Data Migration 18](#_Toc352757760)

[4.2.12 Development toolkit support 18](#_Toc352757761)

[4.3 Software Technology Demonstration and Transition 18](#_Toc352757762)

[4.4 Test & Evaluation (T&E) 18](#_Toc352757763)

[4.5 Independent Verification and Validation (IV&V) 18](#_Toc352757764)

[4.6 Enterprise Network 18](#_Toc352757765)

[4.6.1 Systems/Network Administration 18](#_Toc352757766)

[4.6.2 Network and Telecommunications Infrastructures 19](#_Toc352757767)

[4.7 Enterprise Management Framework: 20](#_Toc352757768)

[4.8 Cyber Security 20](#_Toc352757769)

[4.8.1 Information Assurance (IA) 20](#_Toc352757770)

[4.8.2 Logical Security 20](#_Toc352757771)

[4.8.3 Certification and Accreditation 21](#_Toc352757772)

[4.8.4 Security Operating Support 21](#_Toc352757773)

[4.9 Operations and Maintenance (O&M) 21](#_Toc352757774)

[4.9.1 Systems Administration 21](#_Toc352757775)

[4.9.2 Network Administration 22](#_Toc352757776)

[4.9.3 Application Support 22](#_Toc352757777)

[4.9.4 Hardware Support 22](#_Toc352757778)

[4.9.5 Security Management 22](#_Toc352757779)

[4.9.6 Disaster Recovery and Continuity of Operations 22](#_Toc352757780)

[4.9.7 Capacity/Availability Planning and Management 22](#_Toc352757781)

[4.9.8 Service/Help Desk/Call Center support 22](#_Toc352757782)

[4.9.9 License Maintenance 23](#_Toc352757783)

[4.9.10 Service Level Agreements 23](#_Toc352757784)

[4.9.11 Database and Data Warehouse Administration 23](#_Toc352757785)

[4.9.12 Data Center Administration 23](#_Toc352757786)

[4.10 Training 24](#_Toc352757787)

[4.11 Information Technology (IT) Facilities 24](#_Toc352757788)

[4.11.1 Incidental Facility Design and Modification Services 24](#_Toc352757789)

[4.11.2 Site Surveys 24](#_Toc352757790)

[4.11.3 Facility Cabling 25](#_Toc352757791)

[4.11.4 Installation 25](#_Toc352757792)

[4.11.5 Physical Security Systems 25](#_Toc352757793)

[5.0 DELIVERABLES 25](#_Toc352757794)

[5.1 Products 25](#_Toc352757795)

[5.2 Data 25](#_Toc352757796)

[6.0 SECURITY 25](#_Toc352757797)

[6.1 Information Security and Privacy Security Requirements: 25](#_Toc352757798)

[6.2 Personnel Security Requirements 26](#_Toc352757799)

[6.3 Facility/Resource Provisions 27](#_Toc352757800)

[6.4 Badges 27](#_Toc352757801)

[6.5 Classified Work 27](#_Toc352757802)

[7.0 CONTRACT MANAGEMENT 28](#_Toc352757803)

[7.1 Government Support 28](#_Toc352757804)

[7.1.1 Task Order Contracting Officer’s Representative (COR) 28](#_Toc352757805)

[7.2 Contractor Program Management 28](#_Toc352757806)

[7.2.1 Work Control 28](#_Toc352757807)

[7.3 Pre-Award Procedures 28](#_Toc352757808)

[7.3.1 Request for Task Execution Plan (RTEP) Process 28](#_Toc352757809)

[7.3.2 Task Execution Plan (TEP) 29](#_Toc352757810)

[7.3.3 TEP Evaluation 32](#_Toc352757811)

[7.4 Issuance of Task Orders 32](#_Toc352757812)

[7.5 Logical Follow-Ons 32](#_Toc352757813)

[7.6 Post Award Procedures 32](#_Toc352757814)

[7.6.1 Request For Post Award Action 32](#_Toc352757815)

[7.6.2 Revised Task Execution Plan for Post Award Actions 33](#_Toc352757816)

[7.6.3 Post Award Action Approval 33](#_Toc352757817)

[8.0 REPORTING AND MEETING REQUIREMENTS 33](#_Toc352757818)

[8.1 Reporting Requirements 33](#_Toc352757819)

[8.1.1 Contractor’s Progress, Status and Management Report 33](#_Toc352757820)

[8.1.2 Contract Performance Report (CPR) 34](#_Toc352757821)

[8.1.3 Status of Government Furnished Equipment (GFE) Report 35](#_Toc352757822)

[8.1.4 Personnel Contractor Manpower Report 35](#_Toc352757823)

[8.2 Meetings and Reviews 36](#_Toc352757824)

[8.2.1 Project Office Initial Program Review (IPR) 36](#_Toc352757825)

[8.2.2 Post-Award Conferences 36](#_Toc352757826)

[8.2.3 Monthly Program Reviews 36](#_Toc352757827)

[8.2.4 Quarterly Prime Program Reviews 36](#_Toc352757828)

[ADDENDUM A 37](#_Toc352757829)

[ADDENDUM B 41](#_Toc352757830)

# SCOPE

This Performance Work Statement (PWS) establishes the requirements for Contractor-provided solutions in support of Information Technology. The Contractor shall provide a total IT services solution encompassing, but not limited to software and IT products incidental to the solution, in conjunction with all services needed to integrate a system, network, or other IT service in order to meet a client’s mission requirements. Accordingly, Task Orders may include acquisitions of software and IT products. Transformation Twenty-One Total Technology (T4) 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. Services shall include technical, systems engineering and other solutions encompassing the entire range of IT requirements. Services, as well as related IT products, may encompass the entire life-cycle of a system, including but not limited to program management and strategy planning, systems/software engineering, enterprise network, cyber security, operation and maintenance and IT facilities. 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.

Contractor-provided solutions may support the Department of Veterans Affairs (VA) and its joint initiatives, other Federal Agencies, and if so authorized by specific Legislation (e.g. Public Law 108-136 Section 803), tasks for State and local Governments involving information technology and telecommunications that are federally funded.

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 multiple functional areas to provide the total life cycle solution.

# 2.0 APPLICABLE DOCUMENTS

Applicable documents are 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 0710 Personnel Security and Suitability Program dated May 18, 2007 (https://www.voa.va.gov/)
9. Department of Veterans Affairs (VA) Directive 6102 (Internet/Intranet Services) (https://www.voa.va.gov/)
10. Department of Veterans Affairs (VA) Handbook 6102 (Internet/Intranet Services) (https://www.voa.va.gov/)
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 Security Handbook 1600.01, Business Associate Agreements (https://www.voa.va.gov/)
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. Department of Veterans Affairs (VA) Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
21. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
22. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010.
23. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
24. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.
25. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle,” March 22, 2010
26. VA Handbook 6500.6, “Contract Security,” March 12, 2010
27. Office of Information and Technology (OI&T) ProPath Process Methodology (<https://www.voa.va.gov/>) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
28. National Institute of Standards and Technology (NIST) Special Publication 800-53, “Recommended Security Controls for Federal Information Systems and Organizations” (https://www.voa.va.gov/)
29. Project Management Accountability System (PMAS) portal (https://www.voa.va.gov/)
30. Federal Travel Regulation (FTR) (www.gsa.gov/federaltravelregulation)
31. Technical Reference Model (TRM) (<https://www.voa.va.gov/>)
32. Federal Segment Architecture Methodology (FSAM) v1.0, December 2008
33. National Institute Standards and Technology (NIST) Special Publications 800 series
34. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
35. VA Directive 6300, Records and Information Management, February 26, 2009
36. VA Directive 6300, Records and Information Management, February 26, 2009
37. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010

OMB Memorandum, “Transition to IPv6”, September 28, 2010

# 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 Time-and-Materials (T&M), Cost Reimbursement (CR), and/or Firm-Fixed-Price (FFP) basis.

## 3.2 Period of Performance

The period of performance for the basic contract shall be five (5) years from the effective date of award.

Work at a Government site shall not take place on Federal holidays or weekends (but may require off-hour work due to network loading or other disruptions that could occur) unless directed by the Contracting Officer (CO). The Contractor may also be required to support 24/7 operations 365 days per year as identified in individual Task Orders.

## 3.3 Place of Performance

The place of performance shall be identified in individual Task Orders. Locations will be Government or Contractor sites within the continental United States (CONUS) and/or outside the continental United States (OCONUS). Locations may include Federal, State, VA, or military data centers, facilities, treatment facilities, health clinics and Tricare facilities as defined in individual Task Orders.

## 3.4 Travel

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

## 3.5 Materials, Equipment and Facilities

### 3.5.1 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.

### 3.5.2 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 in accordance with Government direction. See Section 6.0 for detailed security requirements.

### 3.5.3 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.

### 3.5.4 Connectivity

VA will provide the Contractor use of Virtual Private Network (VPN) as appropriate. VA may install equipment at the Contractor’s site to ensure security requirements are in place. The Contractor will bear the cost to provide connectivity to VA through VPN, and VA will provide the required account access accordingly. Other connectivity to VA systems may be authorized as appropriate in individual Task Orders.

### 3.5.5 Facilities

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

#### 3.5.5.1 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 facilities and shall comply with VA and/or Federal certification and accreditation requirements. Such facilities shall be specified in the individual Task Order.

#### 3.5.5.2 Contractor Facilities

Personnel may perform at a Contractor facility or remote locations. Contractors may be required to establish operations and support Contractor facilities and shall comply with VA and/or Federal certification and accreditation requirements. Such facilities shall be specified in the individual Task Order. The Contractor shall disclose this information during the Request for Task Execution Plan (RTEP) process.

### 3.5.6 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.

### 3.5.7 Marking, Handling, Storage, Preservation, Packaging, & Shipping

The Contractor shall establish/maintain procedures for handling, storage, preservation, packaging, and shipping to protect the quality of products and prevent damage, loss, deterioration, degradation or substitution of products.

### 3.5.8 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 in accordance with 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). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 <http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using native IPv6 operations. Information concerning IPv6 transition in addition to OMB/VA Memoranda can be found at <https://www.voa.va.gov/>.

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 9 and Microsoft Office 2010.  However, the migration from Windows XP to Windows 7 is not yet complete within all of VA.  As a result, compatibility with and support on Windows XP, Internet Explorer 7 and Microsoft Office 2007 are also required until April 2014 when Microsoft’s extended support for Windows XP ends.  Applications delivered to the VA and intended to be deployed to Windows XP or 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 VA trusted 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 has been configured using the Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

For VA specific task orders, the Contractor shall support VA efforts in accordance with 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 initiative 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.

Additional frameworks may be specified in individual task orders.

## 3.9 Commercial Development Methodologies

The Contractor may support a Service-Oriented Architecture (SOA) that is a flexible set of [design](http://en.wikipedia.org/wiki/Systems_design) principles used during the phases of [systems development](http://en.wikipedia.org/wiki/Systems_development) and [integration](http://en.wikipedia.org/wiki/Systems_integration). 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.

The Contractor may support a cloud computing environment. Cloud computing is a delivery model for IT services based on the Internet, typically involving the provision of dynamically [scalable](http://en.wikipedia.org/wiki/Scalability) and often [virtualized](http://en.wikipedia.org/wiki/Virtualization) resources [as a service](http://en.wikipedia.org/wiki/Everything_as_a_service) over the [Internet](http://en.wikipedia.org/wiki/Internet). Cloud computing delivers common [business applications](http://en.wikipedia.org/wiki/Business_application) online which are accessed from a [web browser](http://en.wikipedia.org/wiki/Web_browser), while the [software](http://en.wikipedia.org/wiki/Software) and [data](http://en.wikipedia.org/wiki/Data) are stored on [servers](http://en.wikipedia.org/wiki/Server_(computing)). These applications are broadly divided into the following categories, but not limited to [Software as a Service](http://en.wikipedia.org/wiki/Software_as_a_Service) (SaaS), [Utility Computing](http://en.wikipedia.org/wiki/Utility_Computing), Web Services, [Platform as a Service](http://en.wikipedia.org/wiki/Platform_as_a_Service) (PaaS), [Managed Service Providers](http://en.wikipedia.org/wiki/Managed_services#Managed_services_provider) (MSP), Service Commerce, and Internet Integration.

Additional methodologies may be specified in individual task orders.

## 3.10 Integrated 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 (SEI) Capability Maturity Model Integration (CMMI) Level, ISO/IEC 20000, IEEE 1012, or ISO 9001:2008. 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 (not older than three years), 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 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 to Government or Contractor personnel.

# 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).

## 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, 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 and objectives 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. Contractor personnel performing such services shall be required to sign a non-disclosure agreement. 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 not limited to:

1. Enterprise analysis
2. Business and Application architecture
3. Business Process Reengineering
4. Feasibility studies
5. Requirements planning and management
6. Requirements gathering
7. Use Case development
8. Agile requirements methods
9. Requirements analysis
10. Change management
11. Peer Reviews
12. Solution Assessment and Validation
13. Business Process Modeling

#### 4.1.3.1 Requirements Packages

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

1. Assistance in developing Statements of Objectives, Statements of Work, Performance Work Statements, Performance Specifications, Rough Orders of Magnitude (ROM), cost estimates, Quality Assurance Surveillance Plans, and associated acquisition documentation
2. Technical advice and assistance regarding proposal evaluation
3. 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 not limited to logistics/supportability, engineering, financial, operational, and business processes. 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 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. The Contractor shall support project management functions and reporting which include, but not limited to:

1. Project Planning
2. Schedule Management
3. Financial Management
4. Earned Value Management (EVM)
5. Quality Management
6. Resource Management
7. Requirements Management
8. Communications Management
9. Project Change Management
10. Risk Management
11. Performance Management
12. Knowledge Management (KM)
13. Asset Management

### 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, including engineering drawings, specifications, software configuration documentation, interface control documentation, 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. Product Data may include, but not limited to:

1. Complete design disclosure
2. Form, fit and function requirements
3. Performance specifications

### 4.1.8 IT Services Management Guidance

The Contractor shall be responsible for recommending and supporting the development of IT service management plans, practices, infrastructures and systems utilizing industry best practices to minimize negative impact on the IT enterprise. IT services management includes, but not limited to:

1. Change Management
2. Release Management
3. Configuration Management
4. Incident Management
5. Problem Management
6. Service Desk Management
7. Availability Management
8. Capacity Management
9. Event Management
10. Data & Storage Management
11. Information Technology Infrastructure Library (ITIL)

### 4.1.9 Development Toolkit Guidance

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 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) 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 not limited to planning, requirements analysis, design, coding and unit testing, system integration testing, implementation, maintenance and updating of systems, applications, and/or services. This includes, but not limited to healthcare 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 the Enterprise Architecture and Technical Reference Model, 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:

1. Develop the architecture, common infrastructure and services needed to support systems development (e.g. Service Oriented Architecture)
2. Use common infrastructure and services to minimize the effort required to deliver new functional capabilities at a lower cost
3. Retire older systems and build new systems that are scalable and extensible by building them based on reusable services on commodity IT products
4. 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 to minimize negative impact on the IT enterprise. IT services management includes, but not limited to:

1. Change Management
2. Release Management
3. Configuration Management
4. Incident Management
5. Problem Management
6. Service Desk Management
7. Availability Management
8. Capacity Management
9. Event Management
10. Data & Storage Management
11. Information Technology Infrastructure Library (ITIL)

### 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 information technology 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 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. This may also include secure mobile extensions of these applications.

### 4.2.6 Human-Computer Interaction

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

### 4.2.7 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.

### 4.2.8 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. The level and type of modeling and simulation support required will be specified in the individual task order.

### 4.2.9 Informatics Services

The Contractor shall provide the following informatics services to include, but 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, collaboration tools and software, exchanging information and integrating systems and using data and KM. 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

The Contractor shall develop, recommend, and implement KM strategies, policies, procedures, and best practices. The Contractor shall identify authoritative sources because the contractor shall educate senior management on the benefits and use of KM and conduct training on incorporating KM into daily business processes.

### 4.2.10 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.

### 4.2.11 Current System and Data Migration

These systems are in various stages of the lifecycle from Concept Exploration through and including Production and Deployment. 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.

### 4.2.12 Development toolkit support

The Contractor shall provide services that may include, but 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, 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 Test and Evaluation (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 in accordance with 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 review, evaluate, validate and verify 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 information technology equipment currently within, or under consideration for procurement by VA, or other agency. This includes, but 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 delivering solutions up to turn-key communications systems. This may include, but 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.

#### 4.6.2.1 Data Communications Systems

The Contractor shall provide services related to designing, delivering and maintaining solutions for both secure and non-secure data communications systems which may include 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 premise, beyond the carrier demarcation point.

#### 4.6.2.2 Voice Systems

The Contractor shall provide services related to designing, delivering and maintaining 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 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 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 and maintaining 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 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 over fiber optics, coaxial cable or twisted pair copper cable. The Contractor shall provide technical support for web-based collaboration training and other advanced VTC solutions.

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

The Contractor shall provide services related to designing, delivering and maintaining solutions for both secure and non-secure turn-key LAN and WAN systems and components. This may include, but not limited to engineering, furnishing, installing, testing, operating and maintaining 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 not limited to routers, Ethernet switches, multiplexers – Synchronous optical networking (SONET), Dense Wavelength Division Multiplexing (DWDM), network test equipment, network management systems.

#### 4.6.2.5 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 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 enterprise management framework, to include, but not limited to:

1. 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
2. Performance, Functionality and Validation testing and documentation of technologies (for example: WAN optimization, thin computing, virtualization, de-duplication, Virtual Desktop Infrastructure (VDI))
3. Testing which may involve the comparison of multiple technology vendors in support of a specific technology direction
4. Evaluation of the emerging technologies that enable organizational efficiencies
5. Development of solution driven architecture
6. Analysis and review of proposed solutions (internal and external) for technical merit and compliance to Organizational Technical Standards and published Standards

## 4.8 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 in accordance with 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).

### 4.8.1 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, accreditation/certification, Program Protection Plan (PPP) evaluation, and other cyber security related activities and mandates.

### 4.8.2 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.

### 4.8.3 Certification and Accreditation

The Contractor shall obtain commercial and/or organization specific certifications/authorizations for new or modified systems, applications, designs, equipment or installations in accordance with applicable organization standards specified by individual Task Orders. Specific activities include, but 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.

### 4.8.4 Security Operating Support

The Contractor shall provide operations support for Security Services including, but not limited to Intrusion Detection Systems (IDS) and Intrusion Prevention Service (IPS), Security Device Monitoring, 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 not limited to Managed Firewall Service (MFS), Web Content filtering monitoring, Virtual Private Network (VPN) 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.

## 4.9 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 production environments. This 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. Environments requiring O&M tasks may include pre-production, production, test, training, disaster recovery/fail over, or any other combination of IT accounts. The Contractor may also be required to provide software, 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.

### 4.9.1 Systems 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.

### 4.9.2 Network Administration

The Contractor shall support local area network (LAN), virtual private network (VPN), and Wide Area Network (WAN).

### 4.9.3 Application Support

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

### 4.9.4 Hardware Support

The Contractor shall install, configure, patch, repair, upgrade, or remove servers, server components and operating systems.

### 4.9.5 Security Management

The Contractor shall provide services for certification and accreditation, IT security awareness, information protection awareness, organizationally mandated audit preparation, security test and evaluations, and vulnerability analysis and testing.

### 4.9.6 Disaster Recovery and Continuity of Operations

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.

### 4.9.7 Capacity/Availability Planning and Management

The Contractor shall perform analysis to ensure that IT capacity meets current and future business requirements in a cost-effective manner. The Contractor shall monitor availability and maintenance obligations to sustain IT service-availability to support business in a cost-effective manner.

### 4.9.8 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 not limited to individual computer and peripheral maintenance and desk side services.

### 4.9.9 License Maintenance

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

### 4.9.10 Service Level Agreements

The Contractor shall manage organizational Service Level Agreements (SLA) including, but not limited to developing and monitoring SLA metrics, and establishing escalation procedures. The Contractor may be subject to Service Level Agreements (SLAs) and subsequent metrics as specified in the individual task orders. SLAs may include definitions of services, performance measurement, problem management, customer duties, warranties, disaster recovery, and other common elements. The Contractor may assist in the creation of SLAs with both internal and external stakeholders as well as third-party vendors.

### 4.9.11 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 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 not limited to product recommendation, selection, implementation, dashboard and report development, BI strategies and data/report distribution.

The Contractor may also be required to meet broad-based interoperability requirements at the Federal, state and local level.

### 4.9.12 Data Center Administration

The Contractor shall provide continuous 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.

## 4.10 Training

The Contractor shall identify training requirements, obtain or develop training programs and conduct training for systems, applications and products at any stage of the lifecycle. This includes, but not limited to 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 (IT) Facilities

The Contractor shall provide a total IT solution to the client to include incidental facility design and modification services, conducting site surveys, facility cabling, 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 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 6 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 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 not limited to fully developed and dimensioned floor plan layouts, bills-of-material, telecommunications pathways and spaces, 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 Cabling

The Contractor shall provide expertise in the design and installation of IT distribution systems which may include, but 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, 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 **t**he 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 preliminary and final deliverables and all associated working papers, application source code, and other material deemed relevant by the Government which has been generated by the Contractor in performance are the exclusive property of the Government or as specified in the individual task order. Request for deviation shall be approved by the CO. Data rights for all final deliverables and working papers shall be in accordance with the individual task order.

# 6.0 SECURITY

## 6.1 Information Security and Privacy Security Requirements:

The Contractor shall comply with the VA security requirements in accordance with (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 computer systems shall be subject to background investigations and must receive a favorable background investigation from VA.

The position sensitivity risk designation [LOW, MODERATE, HIGH] and level of background investigation [National organization Check with Written Inquiries (NACI), Moderate Background Investigation (MBI), and/or Background Investigation (BI)] 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 in accordance with VA Directive and Handbook 0710, “Personnel Suitability and Security Program”.

1. 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.
2. The Contractor shall bear the expense of obtaining background investigations.
3. Within 3 business days after award, the Contractor shall provide electronically a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor’s Full Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (Refer to Section 4.6 of the Task Order PWS for investigative requirements by task).
4. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
5. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
6. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP), identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
7. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
8. 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.
9. 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).
10. 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.
11. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

All Contractor personnel who require access to Department of Defense (DoD) computer systems or facilities shall be subject to background investigations and must receive a favorable clearance from DoD. The investigative history for Contractor personnel working under the Task Order must be maintained in the database of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the Contractor use a vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct investigations. For DoD efforts, additional security clearance requirements will be identified at the TO order level.

## 6.3 Facility/Resource Provisions

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will 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. 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 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. For detailed Security and Privacy Requirements refer to ADDENDUM A and ADDENDUM B.

## 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 Government program manager, 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 as required by the Task Order. Contractors must have the appropriate clearances for proposal purposes at the Task Order level.

# 7.0 CONTRACT MANAGEMENT

## 7.1 Government Support

### 7.1.1 Task Order Contracting Officer’s Representative (COR)

A COR shall be designated for each Task Order and shall reside within the Requiring Activity. 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, among others as required to accomplish each Task Order. Contract surveillance duties shall be defined and accomplished in accordance with the Performance Assessment Plan and, if a unique plan is required, the Task Order Quality Assurance Plan shall take precedence.

**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 Acquisition Rapid Response Service (ARRS) 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 2003® family of products, and Microsoft XP® network protocols. The Government shall designate a standard naming convention for all electronic submissions within 60 days after contract award. An interactive portal concept is envisioned 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 VA TAC website 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 in accordance with 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 in accordance with the format provided below unless otherwise specified by the CO. The following information shall be provided and submitted into the VA Acquisition Task Order Management System (ATOMS) portal:

1. In addition to the information requested in the RTEP, the following shall be addressed in every TEP:
2. Proposal Summary Volume including:
3. Task number
4. Date submitted
5. Contractor’s name
6. Contractor task leader contact information for questions
7. Subcontractor and vendors shall be identified by name at all tiers (as applicable)
8. Proposed start and finish dates
9. Proposed total price/cost \*
10. 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.
11. If applicable, FAR 52.244-2 Subcontracts shall be addressed
12. If the prime subcontracts 70% or greater, the prime shall provide a value-added statement for the proposed prime dollars in accordance with FAR 52.215-23
13. Duration for which proposal is valid (minimum 60 days)
14. 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
15. Acknowledgement of Amendments
16. The following shall be addressed only for T&M tasks:
17. 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, ODCs, 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
18. If you intend to propose vendors’ services in your TEP under ODCs, 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). Vendors or subcontractors shall be identified at all tiers
19. The Labor Categories submitted shall reference the Government designated numbering scheme in the Labor Category Description Attachment 003.
20. When both the Prime and/or Subcontractor bid the Program Manager and/or Project Director, labor categories, detailed rationale shall be provided
21. Material costs shall indicate raw material costs and material handling charges, as applicable. The nature and cost associated with each Other Direct Costs (ODC) shall be described
22. Bill of materials, indicating the source, quantity, unit cost and total cost for all required materials
23. 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
24. The Contractor shall submit a completed Section B including all line items for base period and any options
25. The following shall be addressed only for FFP tasks:
26. 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
27. The Contractor shall submit a completed Section B including all priced line items for base period and any options
28. “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)
29. The following shall be addressed only for CR tasks:
30. 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
31. If you intend to propose vendors’ services in your TEP under ODCs, 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). Vendors or subcontractors shall be identified at all tiers
32. The Labor Categories submitted shall reference the Government designated numbering scheme in the Labor Category Description Attachment 003
33. Material costs shall indicate raw material costs and material handling charges, as applicable. The nature and cost associated with each ODC shall be described
34. Bill of materials, indicating the source, quantity, unit cost and total cost for all required materials
35. The Contractor shall notify the Government when using Department of Labor (DoL) labor categories. The notice shall provide the county and state the work is being performed in, and what labor categories are bid
36. “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
37. The Contractor shall submit a completed Section B including all line items for the base period and any option periods.
38. The following pertains to the preparation and submission of all TEPs:
39. Contractors are NOT to submit past performance as a part of their TEP, unless specified in the RTEP.
40. Task Orders are performance based and the Contractor's performance shall be assessed in accordance with the VA TAC Performance Assessment Plan (PAP), Attachment 012. The method of assessment shall be a quarterly client survey completed by the COR, covering achievement of milestones in the following areas, as applicable:
    1. Meeting Technical Needs
    2. Project Milestones and Schedule

* 1. Project Staffing
  2. Value of the Contractor

1. TEP Format

a. Proposal Summary

i Microsoft Word or PDF format

b. Technical Volume

1. Microsoft Word or PDF format
2. No marketing materials; information relevant to the requirement only

c. Cost

1. Shall be provided in Microsoft Excel
2. (T&M only) All Prime, Subcontractor and Vendor Labor costs, Material costs, Travel, and Other Direct Costs (ODC) must be broken out

* (MS Excel) Summary Tab for Cost roll-up, and separate Tabs for Base Period and any Option
* Separate tabs for Subcontractors or vendors is desired
* Contractor shall notify the Government when using Department Of Labor (DOL) labor categories. The notice shall provide in what County and State the work shall be performed, and what labor category(s) are bid

1. (Sole Source Cost and Firm, Fixed-price requirements) All Prime, Subcontractor and Vendor Labor costs, Material costs, travel, and ODCs must be broken out per i and ii above
   * + Profit or fee identified as applicable
     + “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)
2. 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. 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.

### 7.3.3 TEP Evaluation

The goal is to evaluate TEP submittals within twelve (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 a non-Government advisor from Massachusetts Institute of Technology Research and Engineering (MITRE) to assist in the evaluation.  The non-Government advisor 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 advisor’s 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 advisor has completed their particular area of evaluation, they will be released from the evaluation process.  The non-Government advisor 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 in accordance with 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 in accordance with (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.

## 7.6 Post Award Procedures

### 7.6.1 Request For Post Award Action

Upon identification of the need for a modification to a Task Order, the Government shall issue a Request for Post Award Action, designated by an action number, to the Contractor. The CO shall designate individuals authorized to issue such requests upon task order award, in writing. The Contractor shall respond to requests from these authorized individuals only. All Contractor correspondence shall reference the Government designated action number. The Government’s Request for Post Award Action does NOT constitute an authorization to start work. A Request for Post Award action may include, but not limited to cost and no cost changes, period of performance extensions, within scope changes, shipping or inspections changes.

### 7.6.2 Revised Task Execution Plan for Post Award Actions

Within seven (7) work days of receipt of the Request for Post Award Action, the Contractor shall submit a Revised Task Execution Plan (TEP), in accordance with the format defined in Section 7.3.2.

### 7.6.3 Post Award Action Approval

The goal is to approve each Revised TEP within five (5) work days of receipt. The Government shall either approve the TEP or enter discussions as soon as practical after TEP receipt. When requested, the Contractor shall provide an updated TEP to address the results of such discussions.

# 8.0 REPORTING AND MEETING REQUIREMENTS

## 8.1 Reporting Requirements

The deliverables defined below are required for the basic contract and each task order. The basic contract report shall be a rollup of each task order and shall be delivered to the T4 Program Office within the TAC. 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. 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 month. The deliverables shall also be forwarded electronically to the ATOMS Portal.

### 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 005, 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.

1. 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. Significant open issues, risk and mitigation action
   8. Summary of issues closed
   9. Meetings completed
   10. Projected meetings
   11. Subcontractor performance – discuss 1st tier Subcontractors and vendor performance
   12. Projected activities for next reporting period
   13. Explanation if the reporting period is over one month
2. For Each Time and Materials Task, indicate:
3. High level summary
4. Expenditures for the reporting period
5. SLIN expenditure
6. Burn rate
7. Percentage of work completed
8. For Each Fixed Price Task indicate:
9. Receiving report submitted
10. Milestone payment schedule
11. For Each Cost Task, indicate:
12. High level summary
13. Expenditures for the reporting period
14. SLIN expenditure
15. Burn rate
16. Percentage of work completed

1. General and Cumulative Performance. Indicate the following:
2. Any general meetings that occurred with Government representatives during the reporting period
3. Total dollars awarded to date (ceiling)
4. 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.

1. For Each Time and Materials Task, indicate:
2. Expenditures for the reporting period by labor, material and ODCs
3. Labor costs shall be broken down by assigned numbering system for contract, Task Order and labor category, entity (Prime or Subcontractor), rates and hours
4. Material costs and ODCs shall be identified by type, and vendor (as applicable), and discussed
5. Total task expenditures for the fiscal year to date, indicated as total, labor, materials and ODCs
6. Total task expenditures since task award, indicated as total, labor, materials and ODCs
7. The Contract Performance Report as set forth in Section J, Attachment 006**,** shall be submitted monthly via the ATOMS portal.
8. For Each Cost Task, indicate:
9. 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.
10. Total task expenditures for the fiscal year to date, indicated as total labor, materials, ODCs, Cost of Money, and fee.
11. Total task expenditures since task award, indicated as total, labor, materials, ODCs, Cost of Money, and fee.
12. The Contract Performance Report as set forth in Section J, Attachment 007,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.

1. Task Order
2. Project Name
3. Type of Equipment
4. Tracking Number
5. Location
6. Value
7. Total Number of Pieces
8. Total Value of Equipment
9. Anticipated Transfer Date to Government
10. Anticipated Transfer Location
11. The Government Furnished Equipment Report as set forth in Section J, Attachment 008,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:

1. Task Order
2. Name
3. Clearance level and/or Status
4. Company name
5. Prime/Subcontractor
6. Labor Category
7. Facility location
8. Tour of Duty Schedules (e.g. Monday through Friday, 9:00 am to 5:00 pm)
9. Project supporting
10. Contractor Rules of Behavior
11. VA Cyber Security Awareness and Rules of Behavior Training
12. Annual VA Privacy Training
13. The Personnel Contractor Manpower Report as set forth in Section J, Attachment 009(basic) and 010 (task order), shall be submitted monthly via the ATOMS portal

## 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 ARRS 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 Monthly Program Reviews

Monthly Program Review Meetings shall be conducted by the VA TAC ARRS and/or designated COR, or Procurement Coordinator 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 Prime Program Reviews

The VA TAC ARRS 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

1. 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 the 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](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.

1. 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.

* 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>

1. 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 are 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: <http://www.section508.gov> and <http://www.access-board.gov/sec508/standards.htm>. 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.

1. 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.
6. 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 toProtected 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:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. 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.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. 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.

# ADDENDUM B

**VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE**

**VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010**

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.

1. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
   1. 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.
   2. 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.
   3. 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.
   4. 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, 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.
   5. 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.
2. VA INFORMATION CUSTODIAL LANGUAGE
3. 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).
4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. INFORMATION SYSTEM DESIGN AND DEVELOPMENT
16. 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*). 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*.
17. 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.
18. 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.
19. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
20. 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*.
21. 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.
22. 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:
       1. The Systems of Records (SOR); and
       2. 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
23. 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.
24. 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.
25. 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.
26. 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*.*
27. 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.
28. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE
    1. 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.
    2. 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.
    3. 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.
    4. 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.
    5. 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.
    6. 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.
    7. 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.
    8. 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:
29. Vendor must accept the system without the drive;
30. 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
31. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
32. 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;
33. 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
34. 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.
35. 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.
36. SECURITY INCIDENT INVESTIGATION
    1. 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.
    2. 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.
    3. 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.
    4. 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.
37. LIQUIDATED DAMAGES FOR DATA BREACH
    1. 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.
    2. 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.
    3. 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:
       3. date of occurrence;
       4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
       5. Number of individuals affected or potentially affected;
       6. Names of individuals or groups affected or potentially affected;
       7. 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;
       8. Amount of time the data has been out of VA control;
       9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
       10. Known misuses of data containing sensitive personal information, if any;
       11. Assessment of the potential harm to the affected individuals;
       12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
       13. 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.
    4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
       1. Notification;
       2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
       3. Data breach analysis;
       4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
       5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
       6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.
38. 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.

1. TRAINING
2. 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 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.]*
3. 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.
4. 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.

**L.6 PROPOSAL SUBMISSION**

1. INTRODUCTION

The offeror’s proposal shall be submitted electronically by the date and time indicated in the solicitation via the Virtual Office of Acquisition (VOA) Portal as set forth below. For Step One, the offeror’s proposal shall consist of two volumes: I - Technical and VI - Solicitation, Offer and Award Documents and Representations/Certifications. For offerors selected to participate in Step Two, the offeror’s proposal shall consist of six volumes: I – Technical, II – Veterans Involvement, III - Past Performance, IV – Small Business Participation Commitment, V – Price, and VI – Solicitation, Offer and Award Documents and Representations/Certifications. The use of hyperlinks in proposals is prohibited. Files shall not contain classified data. File sizes shall not exceed 100MB. The web address for the VOA site is <https://www.voa.va.gov/>. Offerors will be required to be registered users on the VOA website in order to submit proposals. Registration instructions can be found at the VOA website within the T4 Bidder’s Library. For registration or technical issues concerning proposal submission, contact [voahelp@va.gov](mailto:voahelp@va.gov?%20%20%20%20subject=VOA%20Support&). **WARNING: Please do not wait until the last minute to submit your proposals! To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time.** Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

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

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

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

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

**Step One Submission:**

|  |  |  |
| --- | --- | --- |
| **Title** | **File Name** | **Page Limit** |
| **Volume I - Technical** | | |
|  |  |  |
| Subfactor a - Sample Task 1 | (Prime Offeror)\_ ST1.PDF | 25 Page Limit |
| **Volume VI – Solicitation/Amendments and Representations/Certifications** | | |
| Solicitation and any associated amendments, Section J - Attachment 012. | (Prime Offeror)\_OFRREP1.PDF | No Page Limit |

The cover page, table of contents and/or a glossary of abbreviations or acronyms will not be included in the page count of the technical Volume. However, be advised that any and all information contained within any table of contents and/or glossary of abbreviations or acronyms submitted with an offeror’s proposal will not be evaluated by the Government.

(i) VOLUME I – TECHNICAL. This volume shall contain a response to Sample Task 1.

(ii) VOLUME VI – SOLICITATION/AMENDMENTS, REPRESENTATIONS/CERTIFICATIONS.

An authorized official of the firm shall complete and sign the SF33 (to include company name, address, cage code, and telephone number). An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

(a) Solicitation Section A – Standard Form (SF33) and Acknowledgement of Amendments, if any.

(b) Solicitation Section J – Attachment 012. Offeror shall certify that the Sample Task 1 response is the work of the offeror and its proposed subcontractors.  **The Government will not evaluate responses from offerors that do not provide the certification or provide falsified certifications; and all such responses will be deemed ineligible for award**.

**Step Two Submission:**

Note: For those offerors proceeding to Step Two, the Government will allow a 30 day response time for proposal submission.  Sample Task 2 will be released 21 days after the commencement of Step Two, and the response shall be included with the step two proposal submission no later than day 30.

|  |  |  |
| --- | --- | --- |
| **Title** | **File Name** | **Page Limit** |
| **Volume I - Technical** | | |
| Subfactor (a) - Sample Task 2 | (Prime Offeror)\_ST2.PDF | 25  Page Limit |
|  |  |  |
| Subfactor (b) - Management | (Prime Offeror)\_MGMT.PDF | 25 Page Limit |
| **Volume II - Veterans Involvement** |  |  |
| Veterans Involvement | (Prime Offeror)\_VET.PDF | 1 Page Limit |
| **Volume III – Past Performance** | | |
| Section 1 | (Prime Offeror)\_CD.XLS(X) | No Page Limit |
| Section 2 | (Prime Offeror)\_PERF.PDF | 2 Page Limit per instance |
| Section 3 | (Prime Offeror)\_QUESTIONNAIRE.PDF | No  Page  Limit |
| **Volume IV - Small Business Participation Commitment** |  |  |
| Small Business Participation Commitment | (Prime Offeror)\_SBPC.PDF | 15 Page Limit |
| **Volume V - Price** | | |
| Pricing Attachment – CONUS/OCONUS Years 3-5 | (Prime Offeror)\_PRICE .XLS(X) | No Page Limit |
| Pricing Methodology | (Prime Offeror)\_PRMETH.PDF | 3 Page Limit |
| **Volume VI - Solicitation, Offer and Award Documents** | | |
| Solicitation, Offer & Award Documents, Section J - Attachment 014 | (Prime Offeror)\_OFRREP2.PDF | No Page Limit |

(i) VOLUME I – TECHNICAL. This volume shall contain separate responses to Sample Task 2 and Sub-Factor (b) Management as specified in the table above.

(a) The offeror's management proposal shall address the following:

(1) The proposed approach of how the effort required by the T4 PWS will be allocated among the offeror and its proposed subcontractors. The offeror shall provide a brief narrative on the skills/expertise of the prime and each proposed subcontractor. The proposed subcontractors and allocation of work should be consistent between all of the evaluation factors.

(2) The proposed management approach to ensure development of a quality assurance system and processes to capture performance and contract metrics that will ensure execution of individual task orders in accordance with schedule, cost and technical requirements.

(3) The proposed approach to recognize, react to and correct problems, which may arise in the performance of a task order.

(4) The proposed approach to effectively forecast and control costs associated with all T4 contract types, including any special financial tools or methods.

(5) Contractor/Subcontractor Core Competency – The offeror shall provide a brief narrative on its mechanism to attract and retain its workforce.

(ii) VOLUME II – VETERANS INVOLVEMENT.

(a) For SDVOSBs: In order to receive full credit under this Factor, offerors shall submit a statement identifying itself as a SDVOSB. Offerors are cautioned that they must be registered and verified in VIP database (<http://www.VetBiz.gov>) at the time of Step Two proposal submission.

(b) For VOSBs: To receive partial credit under this Factor, offerors shall submit a statement identifying itself as a VOSB. Offerors are cautioned that they must be registered and verified in Vendor Information Pages (VIP) database (<http://www.VetBiz.gov>) at time of Step Two proposal submission.

(iii) VOLUME III – PAST PERFORMANCE. The offeror shall submit Volume III Past Performance Proposal in a separate file. Past performance of the offeror and its proposed three major subcontractors will be evaluated. The three major subcontractors are defined as the three subcontractors expected to receive the highest dollar value of subcontracted work as identified in the offeror’s Price volume. Prime offerors shall submit up to three (major subcontractors shall submit up to two) instances of Government or Commercial contracts (prime contracts, task/delivery orders, and/or major subcontracts in performance during the past three years from the date of issuance of solicitation Step Two), which are relevant to the efforts required by this solicitation. Areas of relevance include contracts greater than $1,000,000 which provide services similar to those required under functional areas 4.1 through 4.11 of the T4 PWS. Data concerning the prime offeror shall be provided first, followed by each proposed major subcontractor, in alphabetical order. The Past Performance volume shall be organized into the following sections:

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

This section shall include the following information:

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

(2) Government contracting activity, and current address, Procuring Contracting Officer's name, e-mail address, and telephone number.

(3) Government’s technical representative/COR, and current e-mail address, and telephone number.

(4) Commercial Contract Point of Contact, Email Address, Tel & Fax Number.

(5) Contract Number and task order number (if applicable), period of performance, and total contract value.

(b) Section 2 - Performance. Offerors shall provide a specific narrative explanation of each contract listed in Section 1 describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation.

(c) Section 3 - Past Performance Assessment Questionnaire. Past Performance Assessment Questionnaires, found at Section J Attachment 015, must be completed and submitted for all contract(s)/task order(s) identified in Section 1.

(iv) VOLUME IV – SMALL BUSINESS PARTICIPATION COMMITMENT.

(a) Offerors are required to submit Small Business Participation Commitment information that shall include the following:

Type of Business of Prime Contractor (check all applicable boxes):

{ } Small (also check type of Small Business below)

{} Small Disadvantaged Business (SBA Certified)

{} Women-Owned Small Business

{} HUB Zone Small Business (SBA Certified)

{} Veteran Owned Small Business

{} Service Disabled Veteran Owned Small Business

{}8(a) Small Business (SBA Certified)

(b) Offerors are required to submit Small Business Participation Commitment information addressing each of the following:

**A**. Summary of Proposed Small Business Goals by Percentage.

|  |  |
| --- | --- |
| **Small Business Category** | **Proposed Goal %** |
| Overall Small Business Participation |  |
| Service Disabled Veteran Owned Small Business (SDVOSB) |  |
| Veteran Owned Small Business (VOSB) |  |
| Small Disadvantaged Business (SDB) (including 8(a)) |  |
| Women-Owned Small Business |  |
| Historically Underutilized Business Zone (HUB Zone) Small Business |  |

**B**. The extent of participation of such firms in terms of the value of the total acquisition. **The sum of the dollars may exceed the total proposed contract value since the offeror and its proposed subcontractors may be counted in more than one category.**

|  |  |
| --- | --- |
| **Description** | **Dollars** |
| A. TOTAL CONTRACT VALUE:  This value should match the TOTAL CONTRACT  VALUE you have proposed in your price proposal volume. |  |
| B. DOLLAR VALUE OF YOUR PARTICIPATION AS PRIME CONTRACTOR: Enter your participation as prime contractor. |  |
| C. DOLLAR VALUE OF SUBCONTRACTS  PLANNED FOR LARGE BUSINESS |  |
| D. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR SMALL BUSINESS:  This is the sum of all subcontracts to Small Business, Small Disadvantaged, Women Owned Small, Hubzone Small, Veteran Owned Small, Service Disabled Veteran Owned Small and HBCU/MI. |  |
| E. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR SMALL DISADVANTAGED BUSINESS (SDB) (including 8(a)) AND HBCU/MI  This should reflect the value of all subcontracts planned for SBA CERTIFIED SDB (as verified in Central Contract Registry-CCR) or HBCU/MI with the exception that ANC and Indian Tribes are exempt IAW 52.219-9(d)(1)(i). |  |
| F. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR WOMEN OWNED SMALL BUSINESS:  This should reflect the value of all subcontracts planned for Women Owned small businesses. |  |
| G. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR HISTORICALLY UNDERUTILIZED BUSINESS ZONE (HUBZONE) SMALL BUSINESS:  This should reflect the value of all subcontracts planned for SBA CERTIFIED HUBZone small businesses as verified in Central Contract Registry- CCR. |  |
| H. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR VETERAN OWNED SMALL BUSINESS:  This should reflect the value of all subcontracts planned for ALL Veteran Owned small businesses including Service-Disabled Veteran-Owned Small Businesses (SDVOSB). |  |
| I. DOLLAR VALUE OF PARTICIPATION/SUBCONTRACTS PLANNED FOR SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS (SDVOSB):  The value of all subcontracts planned for Service-Disabled Veteran-Owned small businesses (SDVOSB). |  |

**C.** The variety of the work proposed subcontractors are to perform.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Company Name** | **Cage Code** | **Business Type** (list all small business categories) | **Dollars** | **NAICS** | **Reference to Paragraph/**  **Section in PWS** (if applicable) | **Type of Agreement** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**D.** The realism of the proposal;

To demonstrate this element, provide narrative information on how goals for this effort were developed, why they are realistic, and the types of agreements (long-term, mentor-protégé, unilateral, bilateral or short-term) maintained with the proposed subcontractors. If applicable, provide detailed mitigation plans and/or narrative explanations as to why certain goals specified by the Government in Section M, Basis for Award cannot be met as reflected in the table above (Element B).

(v) VOLUME V– PRICE. The offeror shall submit a price proposal for a three-year effort in support of the overall contractual requirements to include the following:

(1) For each Government labor category specified in Section J of the RFP, Attachment 001 Labor Category Descriptions, the offeror shall provide the loaded labor rates, and allocate the number of labor hours for the prime and each subcontractor, for each year of the three year ordering period. Labor rates must be provided for On-Site, Off-Site, and OCONUS work locations. On-Site locations are defined as Government owned and/or operated facilities. Off-Site locations are defined as non-Government owned and/or operated facilities (i.e., the offeror’s local work facility, etc.). OCONUS locations are defined as Government owned and/or operated facilities (On-Site) outside the continental United States. The offeror must provide a separate fully loaded rate associated with each labor category for each individual year of the three-year base contract. Rates are to be escalated from year to year as deemed appropriate by the offeror. For evaluation purposes, the offeror shall use the level of effort estimates set forth in Section J of the RFP. When subcontracted effort is proposed, rates must be clearly distinguished as the contractor’s rate or the subcontractor’s rate. The loaded rates for the prime contractor and each subcontractor will be incorporated into the contract and will include all cost elements as specified in FAR 52.232-7(a). For the prime contractor and each subcontractor, only those labor categories which have hours proposed for them in the proposal will be included in the contract. The apportionment of hours should reflect a realistic assessment of each team member’s expected participation/contribution to the effort. Offerors are cautioned to ensure that the allocation of work among the prime contractor and the subcontractors indicated in the Price proposal corresponds to the distribution of work indicated in the Management Past Performance and Small Business Participation Commitment volumes. Each labor category specified by the Government in the RFP must be addressed by either the prime, at least one of the subcontractors or both (i.e., no un-addressed labor categories). The offeror is required to provide and pay for its employees’ personal computer equipment, phones and calls, copiers, fax machines, office supplies, mail costs, etc. utilized while at Off-Site work locations. The cost for these items shall be incorporated into the overhead cost or G&A that is included in the proposed loaded hourly rates and will not be allowed as ODCs in task orders. The offeror shall use the format as depicted in the Excel spreadsheets set forth in Section J of the RFP.

(2) The offeror is required to include the Government-provided Material/ODC amount and the Government-provided Travel amount plus applicable Material Handling and/or G&A costs as authorized by FAR 52.232-7 (b) (5), Payments under Time and Materials and Labor Hour Contracts for each of the three years of the basic contract. THIS IS AN ESTIMATE FOR EVALUATION PURPOSES ONLY. In accordance with regulations regarding time-and-material contracts, when loading these estimates, no fee is allowed. Expenses for local travel (i.e., from the contractor’s local place of business to the local Government facility) will not be reimbursed as a direct cost.

(3) Labor rates shall be based on an eight-hour workday, forty-hour workweek, and a 1920-hour productive work year. Labor rates and indirect rates shall be no more than two decimal places. Contractors shall be responsible for ensuring compliance with the Service Contract Act (SCA) for applicable Labor Categories.

(4) Allowable loadings specified in FAR 52.232-7(b) (5), Payments under Time and Materials and Labor Hour Contracts, may be added and must be specified. If not included in the proposal, they may not be added during contract performance. The Government will not pay subcontractor rates greater than those contained in the contract.

(5) The Pricing Attachment file shall contain Labor Hours and Loaded Rates per Labor Category for each member of the offeror’s team for both CONUS and OCONUS rates (Worksheet provided in Section J, Attachment 002 of the RFP).

(6) The price proposal shall also include an additional file (PRMETH.PDF) that identifies the offeror’s proposed fringe rate, overhead rate, G&A rate, Facilities Capital Cost of Money rate (if applicable), and profit percentage. Also, any prime contractor loadings (i.e. subcontractor handling, G&A, profit, etc.) to subcontractor loaded labor rates shall be identified. In addition, the offeror’s proposed labor escalation shall be provided for each year. The price methodology file shall be used in accordance with H-6, Consent To Add/Delete Subcontractors.  This will not be evaluated.

(vi) VOLUME VI - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS.

Certifications and Representations - An authorized official of the firm shall sign the SF 33 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

(1) Solicitation Section A – Standard Form SF33 and Acknowledgement of Amendments, if any.

(2) Solicitation Section K – Representations, Certifications and Other Statements of Offerors.

(3) Any proposed exceptions to solicitation terms and conditions. Offerors are hereby advised that any offeror-imposed terms and conditions which deviate from the Government’s material terms and conditions established by the Solicitation, may render the offeror’s proposal Unacceptable, and thus ineligible for award.

(4) Solicitation Section J – Attachment 014 Offeror shall certify that the Sample Task 2 response is the work of the offeror and its proposed subcontractors.  **The Government will not evaluate responses from offerors that do not provide the certification or provide falsified certifications; and all such responses will be deemed ineligible for award**.