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

1. REQUISITION NO.	PAGE 1 OF 72

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NO.	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			36C10B20Q0035	November 13, 2019

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NO. (No Collect Calls)	8. OFFER DUE DATE/LOCAL TIME
	David Melton	732-795-1143	November 20, 2019 10:00AM EST

9. ISSUED BY CODE

Department of Veterans Affairs
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

10. THIS ACQUISITION IS

- [ ] UNRESTRICTED OR [X] SET ASIDE: 100 % FOR:
- [X] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8(A)

NAICS: 541519

SIZE STANDARD: $30 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
[ ] SEE SCHEDULE	N/A	[ ]	N/A [X] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE

See Delivery Schedule

16. ADMINISTERED BY CODE

Department of Veterans Affairs
Office of Acquisition Operations
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

17a. CONTRACTOR/OFFEROR CODE FACILITY CODE

TELEPHONE NO. DUNS: DUNS+4:

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

18a. PAYMENT WILL BE MADE BY CODE

Department of Veterans Affairs

Financial Services Center
PO Box 149971
Austin TX 78714-8971

PHONE: FAX:

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Veteran-facing Services Platform Content Management System POCs: David Melton, Contract Specialist, 732-795-1143, David.Melton@va.gov and Joshua Cohen, Contracting Officer, 732-440-9696, Joshua.Cohen2@va.gov Terms and conditions of the Offeror's GSA Schedule contract shall apply to the solicitation and resultant Order (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)

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

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

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

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)	31c. DATE SIGNED
		Joshua Cohen Contracting Officer	

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto, as permitted by FAR 12.212. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (*e.g*., restricted computer software) are included and made a part of this Contract/Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 *et seq*.), the Anti-Deficiency Act (31 U.S.C. § 1341 *et seq*.), the Competition in Contracting Act (41 U.S.C. § 3301 *et seq*.), the Prompt Payment Act (31 U.S.C. § 3901 *et seq*.), Contracts for Data Processing or Maintenance (38 USC § 5725), and FAR clauses 52.212-4, 52.227-14, 52.227-19 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ) in accordance with 28 U.S.C. § 516; at the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by modification (Standard Form 30) and shall only be made by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.2 SOFTWARE LICENSE, MAINTENANCE AND TECHNICAL SUPPORT:

(1). Definitions.

a) Licensee. The term "licensee" shall mean the U.S. Department of Veterans Affairs ("VA") and is synonymous with "Government."
b) Licensor. The term "licensor" shall mean the Contractor having the necessary license or ownership rights to deliver license, software

maintenance and support of the computer software being acquired. The term "Contractor" is the party identified in Block 17a on the SF1449. If the Contractor is a reseller and not the Licensor, the Contractor remains responsible for performance under this Contract/Order.

c) Software. The term "software" shall mean the licensed computer software product(s) cited in the Schedule of Supplies/Services.
d) Maintenance. The term "maintenance" is the process of enhancing and optimizing software, as well as remedying defects. It shall include all new fixes, patches, releases, updates, versions and upgrades, as further defined below.
e) Technical Support. The term "technical support" refers to the range of services providing assistance for the software via the telephone, email, a website or otherwise.
f) Release or Update. The term "release" or "update" are terms that refer to a revision of software that contains defect corrections, minor enhancements or improvements of the software's functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.
g) Version or Upgrade. The term "version" or "upgrade" are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

(2). Software License.

a) Unless otherwise stated in the Schedule of Supplies/Services, the Performance Work Statement or Product Description, the software license provided to the Government is a perpetual, nonexclusive license to use the software.
b) The Government may use the software in a networked environment.
c) Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).
d) All limitations of software usage are expressly stated in the Schedule of Supplies/Services and the Performance Work Statement/Product Description.

(3). Software Maintenance and Technical Support.

a) If the Government desires to continue software maintenance and support beyond the period of performance identified in this Contract/Order, the Government will issue a separate contract or order for maintenance and support. Conversely, if a contract or order for continuing software maintenance and technical support is not received, the Contractor is neither authorized nor permitted to renew any of the previously furnished services.
b) The Contractor shall provide software support services, which includes periodic updates, enhancements and corrections to the software, and

reasonable technical support, all of which are customarily provided by the Contractor to its commercial customers so as to cause the software to perform according to its specifications, documentation or demonstrated claims.

c) Any telephone support provided by Contractor shall be at no additional cost.
d) The Contractor shall provide all maintenance services in a timely manner in accordance with the Contractor's customary practice or as defined in the Performance Work Statement or Product Description. However, prolonged delay (exceeding 2 business days) in resolving software problems will be noted in the Government's various past performance records on the Contractor (e.g., www.ppirs.gov).
e) If the Government allows the maintenance and support to lapse and subsequently wishes to reinstate it, any reinstatement fee charged shall not exceed the amounts that would have been charged if the Government had not allowed the subscription to lapse.

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

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

B.3 CONTRACT ADMINISTRATION DATA

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

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

a. CONTRACTOR: TBD

b. GOVERNMENT: Joshua Cohen
Contracting Officer 36C10B
Department of Veterans Affairs
Office of Procurement, Acquisition, and Logistics
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

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

[X] 52.232-33, Payment by Electronic Funds Transfer—System For Award Management, or
[] 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:

a. Quarterly []

b. Semi-Annually []

c. Other [X] In accordance with Section B.4, “Price Schedule”

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

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

AMENDMENT NO	DATE

B.4 PRICE SCHEDULE

Days used below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

BASE PERIOD					
LINE ITEM	**DESCRIPTION**	**QTY**	**UNIT**	**UNIT PRICE**	**TOTAL PRICE**
0001	**TIME AND MATERIAL (T&M) LABOR** In accordance with (IAW) Performance Work Statement (PWS) Paragraphs 5.1 inclusive of all subparagraphs through 5.2 inclusive of all subparagraphs. This is a T&M Contract Line Item Number (CLIN) and includes all labor and deliverables required for the successful completion of the tasks associated with PWS Paragraphs 5.1 inclusive of all subparagraphs through 5.2 inclusive of all subparagraphs. This T&M CLIN is in IAW Paragraph (i) of Federal Acquisition Regulation (FAR) 52.212-4 Alternate I for invoicing or billing purposes. All labor rates shall be in accordance with Attachment 0001. Period of Performance (PoP) shall be 12 months after effective date.	1	LO	Not-To-Exceed (NTE) $	NTE $
0002	**T&M TRAVEL** Travel for the base period in accordance with PWS paragraph 4.3. Travel shall be in accordance with the Federal Travel Regulations (FTR). Travel requires advanced concurrence and shall be approved by the VA Contracting Officer's Representative (COR) in writing. Task order travel within the local commuting area will not be reimbursed. The Contractor's	1	LO	NTE $	NTE $

	fixed handling rate as set forth herein may be applied to the billable travel cost and shall not exceed that set forth in the basic contract. Profit shall not be applied. Government Not to Exceed Travel Ceiling: $43,431.13 + Fixed Handling Rate ___% = Travel NTE Ceiling $_____ (Inclusive of Government NTE travel ceiling + Fixed Handling Rate)				
0003	**T&M MATERIALS** Materials are IAW PWS Paragraph 5.2 This is a T&M CLIN. All Materials purchased under this CLIN must obtain COR approval prior to purchase. Invoicing shall be in accordance with Paragraph (i) of Federal Acquisition Regulation (FAR) 52.212-4 Alternate I Calculated Not to Exceed Ceiling: $700,000.00 + Fixed Handling Rate ___% = Materials NTE Ceiling $_____ (Inclusive of Calculated NTE Material ceiling + Fixed Handling Rate)	1	LO	NTE $	NTE $
				Base Period Total	**$**

OPTION PERIOD 1

THIS OPTION PERIOD MAY BE EXERCISED IAW FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000). WORK SHALL NOT COMMENCE UNTIL, AND UNLESS, A FORMAL MODIFICATION IS ISSUED BY THE CONTRACTING OFFICER. IF EXERCISED, THIS OPTION SHALL COMMENCE IMMEDIATELY AFTER EXPIRATION OF THE BASE PERIOD.

LINE ITEM	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
1001	**Time and Material (T&M) LABOR** In accordance with (IAW) Performance Work Statement (PWS) Paragraphs 5.1 inclusive of all subparagraphs through 5.2 inclusive of all subparagraphs.	1	LO	NTE $	NTE $

	This is a T&M Contract Line Item Number (CLIN) and includes all labor and deliverables required for the successful completion of the tasks associated with PWS Paragraphs 5.1 inclusive of all subparagraphs through 5.2 inclusive of all subparagraphs. This T&M CLIN is in IAW Paragraph (i) of Federal Acquisition Regulation (FAR) 52.212-4 Alternate I for invoicing or billing purposes. All labor rates shall be in accordance with Attachment 0001. Period of Performance (PoP) shall be 12 months after effective date.				
1002	**T&M TRAVEL** Travel for the base period in accordance with PWS paragraph 4.3. Travel shall be in accordance with the Federal Travel Regulations (FTR). Travel requires advanced concurrence and shall be approved by the VA Contracting Officer's Representative (COR) in writing. Task order travel within the local commuting area will not be reimbursed. The Contractor's fixed handling rate as set forth herein may be applied to the billable travel cost and shall not exceed that set forth in the basic contract. Profit shall not be applied. Government Not to Exceed Travel Ceiling: $<u>44,430.05</u> + Fixed Handling Rate ___% = Travel NTE Ceiling $_____ (Inclusive of Government NTE travel ceiling + Fixed Handling Rate)	1	LO	NTE $	NTE $
1003	**T&M MATERIALS** Materials are IAW PWS Paragraph 5.2	1	LO	NTE $	NTE $

	This is a T&M CLIN. All Materials purchased under this CLIN must obtain COR approval prior to purchase. Invoicing shall be in accordance with Paragraph (i) of Federal Acquisition Regulation (FAR) 52.212-4 Alternate I Calculated Not to Exceed Ceiling: $716,100.00 + Fixed Handling Rate ___% = Materials NTE Ceiling $_____ (Inclusive of Calculated NTE Material ceiling + Fixed Handling Rate)				
				Option Period 1 Total	**$**

BASE AND OPTION PERIOD DELIVERABLES

ALL DELIVERABLES LISTED BELOW SHALL BE DELIVERED FOR THE BASE PERIOD AND IF EXERCISED OPTION PERIOD 1

LINE ITEM	DESCRIPTION	QTY	UNIT	UNIT PRICE	TOTAL PRICE
2001AA	**CONTRACTOR PROJECT MANAGEMENT PLAN** IAW PWS Paragraph 5.1.1 Due Thirty (30) days after award effective date (AED) and updated monthly thereafter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination FOB: destination	1	LO	NSP	NSP
2001AB	**MONTHLY STATUS REPORT** IAW PWS Paragraph 5.1.2.2 Due the fifth day of each month throughout the period of performance (PoP). Electronic submission to: VA PM, COR, CO	1	LO	NSP	NSP

	Inspection: destination Acceptance: destination FOB: destination				
2001AC	**TMS TRAINING CERTIFICATES** IAW PWS Paragraph 5.1.3 Due 5 days AED and within 5 days of the onboard of each new employee Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination FOB: destination	1	LO	NSP	NSP
2001AD	**SIGNED CONTRACTOR RULES OF BEHAVIOR** IAW PWS Paragraph 5.1.3 Due 5 days AED and within 5 days of the onboard of each new employee Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination FOB: destination	1	LO	NSP	NSP
2001AE	**CONTRACTOR STAFF ROSTER** IAW PWS Paragraph 6.2.2 *Due 3 days after AED and updated within 1 day of any changes occurring thereafter.* Electronic submission to: VA PM, COR, CO Inspection: destination Acceptance: destination FOB: destination	1	LO	NSP	NSP

B.5 PERFORMANCE WORK STATEMENT (PWS)
DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology
Enterprise Program Management Office

Veteran-facing Services – Content Management System

Date: November 8, 2019
PWS Version Number: 1.0
TAC-20-57507

1.0 BACKGROUND

Every month, over 10 million people access the Department of Veterans Affairs (VA) digital tools and content. Many of these users have a frustrating experience, encountering a complicated ecosystem of websites, forms, logins, brands, and outdated tools. Additionally, the VA is responsible for many legacy systems with varied languages and environments. Every system is different and there is not consistent documentation.

To begin to address these issues, VA's Office of Information & Technology (OI&T) and Digital Service at VA (DSVA) built and launched Vets.gov in November 2015. Vets.gov delivered a modern digital experience that enabled Veterans to learn about, apply for, and manage their VA benefits in an effective, efficient, and compassionate manner.

By December 2016, Vets.gov became the 6th most used VA site. In building and improving Vets.gov, DSVA leveraged the advantages of cloud computing, Platform as a Service, and Infrastructure as a Service, as well as adopted continuous integration and continuous delivery (CI/CD). These various resources, combined with agile, user-centered practices, began to coalesce in a rough product development platform.

To further harmonize Veterans' digital experience, the VA began a project to consolidate the hundreds of VA websites (including Vets.gov) under one VA.gov site. As a result, a much improved VA.gov was launched on Veterans Day 2018, serving millions of visitors per month. This new digital "front door" effort is aligned with the VA's "Digital Modernization Strategy"

In September 2018, VA awarded the initial phase of development for the creation of a Content Management System. The work included:

- Building a new Drupal-based content management system (de-coupled implementation)
- Integration with the existing front end of VA.gov via a content Application Programming Interface (API)
- Developing reusable content models
- Creating content governance, workflows, and permissions
- Supporting and training VA staff

The team successfully migrated the modernized portions of VA.gov to the Drupal Content API. This included the nine 'benefit hubs', the service member and family member hubs, global navigation, and the VA.gov homepage. In addition, the team created a pilot VA Medical Center website for the VA Pittsburgh Health Care System (https://www.va.gov/pittsburgh-health-care/) and a new Office of Public Affairs outreach sub-site (https://www.va.gov/outreach-and-events/) which allowed VA to retire the subdomain explore.va.gov. These are examples of new, Drupal-powered sites on VA.gov which will be the default method for creating Un-authenticated, public-facing portions of the website moving forward.

The subject of this PWS is the continuation of this work. Specifically, additional development and sustainment of the Drupal Content-API, support for the VA Drupal community, and continuous improvement on the Drupal authoring experience.

2.0 WORKING PRINCIPLES AND DEFINITIONS

2.1 WORKING PRINCIPLES

The DSVA/Digital Experience Product Office (DEPO) teams follows the practices described in the "Digital Services Playbook" (https://playbook.cio.gov). Using the Digital Services Playbook, DSVA/DEPO operate with a **user-centered agile delivery process** – learning from research and prototypes, using that knowledge to iteratively design and build digital applications and features for Veterans, and iteratively launching those applications and features on a daily basis.

The Contractor shall follow the same Working Principles to maintain the Content API by iteratively designing and building features and enhancements - launching them on a daily basis.

The Contractor shall:

1. Follow the practices described in the "Digital Services Playbook" (https://playbook.cio.gov). The Contractor shall be familiar with the concepts in each play and implement them in their solutions and support.
2. Incorporate Agile methodology and iteration ceremonies into all work, such as (but not limited to) sprint planning, daily scrum, sprint review, sprint retrospective, backlog grooming, and estimating activities.
3. Incorporate best practices for modern user research and usability testing into all solutions.
4. Actively involve users in the design of all solutions.
5. Maintain a consistent look, feel, and voice across user facing sites and services.
6. Whenever possible, personalize solutions for the individual or teams using the service.
7. Leverage existing VA internal Single Sign On (SSOi) with VA's overall authentication strategy.
8. Optimize web applications for mobile-first operation, with all solutions being equally available on both mobile and desktop.
9. Protect user information with best-in-class security, given the constraints of the environment.
10. Incorporate robust accessibility principles into design, development and testing for all web applications to deliver high-quality digital experiences to users of assistive devices.
11. Design, develop, configure, customize, deploy, and operate these solutions.
12. Use DevOps techniques of continuous integration and continuous deployment across all environments including, at a minimum, development, staging, and production.
13. Deliver secure, scalable, and tested modern web application designs using automated testing frameworks to create unit tests, integration tests, functional/black box tests, and load tests (or their equivalents as applicable) to test 100% of functionality delivered. The Contractor should strive for compliance with Test Driven Development practices.
14. Ensure configuration and sensitive data, including data the VA defines as sensitive, are not present in source code, and are stored in encrypted credential management systems.

15. Deliver all code not containing configuration or sensitive data to an open source repository per OMB Guidance M-16-21.
16. Cultivate positive, trusting, and cooperative working relationships with the government and all other vendors supporting this work.

2.2 DEFINITIONS

1. **DSVA:** The VA U.S. Digital Service team provided the overall strategic direction for the establishment of Veteran-facing Services (VFS) at VA. This team manages designated Veteran-facing Services and communicates with the stakeholder community.
2. **DEPO:** The Digital Experience Product Office was created in 2019 as the first implementation of the new Product Line Management structure for OI&T. DEPO is the new product shop for VA.gov and is responsible for all Veteran-facing Services. Additionally, DEPO:
    a. Is responsible for ongoing delivery and maintenance of the Digital Modernization Strategy
    b. Builds, maintains, and improves the public-facing experience on VA.gov
    c. Provides Veterans, family members, caregivers, service members and other audiences access to vital information about VA benefits and services
    d. Delivers self-service tools, including benefit applications
    e. Gives VA's customers a personalized experience
    f. Provides VA business lines a place to communicate with all their customers about the organization
3. **VFS:** Any application, digital tool, digital form, API, digital migration, or other solution that is released (or planned to be released) on the Veteran-facing Services Platform (VSP).
4. **VSP:** The technical infrastructure and product development processes that support new development (from initial research phases through pre-launch checks) and maintenance of VFS for VA.gov.
    a. Technical infrastructure maintenance and development includes responsibility for the technology that supports existing VFS that were migrated from the Vets.gov domain to the VA.gov domain in November 2018, as well as any future VFS that will be available via the VA.gov domain, whether developed by DSVA or another VA team. These tasks include, but are not limited to:
        - managing infrastructure, networking, and build/deploy processes with infrastructure as code;
        - managing all Authority to Operate (ATO) compliance requirements;
        - maintaining a Rails-based authenticated API layer between applications and VA resources;
        - maintaining automated testing, identity and analytics services;
        - maintaining complete documentation of the VSP;
        - building and maintaining core VA.gov resources, including:
            - reusable React and Redux components;

- a design system based on U.S. Web Design Standards (known as Formation);
- a forms system based on the U.S. Forms System;
- a Drupal based content management system; and
- a static site generator;

- monitoring performance for all VSP applications;
- providing targeted operation and maintenance (sustainment) support for certain VSP applications;
- maintaining consolidated web analytics for all VSP applications;

b. The VSP facilitates the development and delivery of high quality VFS through a wide range of activities including but not limited to:

- For Other VA Product Teams,
  - Supporting standardized checkpoints and reviews with teams to help them achieve quality standards that align with user-centered, agile delivery methodologies for all VSP applications;
  - onboarding and offboarding;
- For all teams,
  - providing close support during application development
  - conducting code, design, content, analytics, and accessibility reviews;
  - conducting load testing;
  - coordinating and preparing call centers for new features
  - enforcing a common information architecture for all VSP applications;

5. **Veteran-facing Services Applications (VSA):** Teams under this contract design and build VFS including public facing webpages/sites and authenticated benefit tools and applications. The VSA Teams coordinate and schedule with the VSP Team to deploy their VFS according to the defined guidelines.

6. **VFS Content Management System (CMS) / Drupal Content API:** The content management system application, administrative interface, GraphQL application interface, and any related configurations and integrations. The Drupal authoring experience and user community management.
   a. The Content API infrastructure is hosted in the VA Enterprise Cloud.
   b. Public documentation: https://github.com/department-of-veterans-affairs/va.gov-cms/blob/master/README.md

7. **Other VA Product Teams:** Teams that design, build, and manage Veteran-facing Services independently of Contractor. Other VA Product Teams coordinate and schedule with Contractor to deploy their Veteran-facing Services according to the guidelines defined for the VSP, including DSVA/DEPO-managed teams.

- **Enterprise Service Desk (ESD):** ESD is the starting point for most VA Employee help desk concerns, they triage tier 1 incidents between the PIV/SSOi team and the CMS team

3.0 SCOPE OF WORK

This Contractor shall support VA in the operation, administration, and improvement of the Drupal-based Content API in accordance with the Working Principles and Definitions provided in Section 2 above.

The Contractor shall provide VA with iterations of agile software delivery. The agile delivery iterations will include product and delivery management, Drupal development, software/API development, user research and design, DevOps, and helpdesk/training support in order to achieve the tasks outlined in Section 5.2.

3.1 ORDER TYPE

The effort shall be proposed on a Time and Materials (T&M) basis. The Contracting Officer reserves the right to negotiate the conversion of this Task Order from the initial T&M type order to a Firm-Fixed-Price (FFP) type order at any time during the base or option period. Conversion of certain tasks to FFP does not require the full Order to be converted and the Government withholds the right to only convert certain tasks to FFP.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

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

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

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

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Efforts under this PWS may be performed in VA facilities located at 811 Vermont Ave NW, Washington, DC and/or at the Contractor's site. The Government will provide up to 6 hoteling spaces for Contractor staff to use throughout the life of the project. The Government strongly recommends that the Contractor maintain regular physical presence on the Government site.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Contractors may be required to perform additional site-visits (CONUS only) to government and non-government facilities to conduct user research or stakeholder engagement

Travel shall be reimbursed on a Time & Materials basis in accordance with the Federal Travel Regulations and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed.

4.4 MATERIALS

The Government anticipates the Contractors need for additional software and tools to be reimbursed on a Time & Materials basis with prior written authorization by the COR. This CLIN includes all materials and deliverables required for the successful completion of the tasks associated with this PWS.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

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

Deliverable:

A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

5.1.2.1 Enterprise Program Management Office (EPMO) MANAGEMENT

The Contractor shall use the DSVA/DEPO's Github environment to track execution details. The Github Repository will be used to provide a single authoritative product data source and artifact repository. The Contractor shall utilize Github tools, at a minimum, to:

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

The Contractor shall use GitHub, GitHub Extensions, and other approved tools to provide full technical and end-user documentation, during and at the end of the project, for all software development efforts and product releases with all information necessary to document processes, procedures, code artifacts, test scripts, and/or policies that were implemented over the course of this contract.

5.1.2.2 MONTHLY STATUS REPORTS

Contractor shall deliver monthly Review Report detailing the status of all work efforts. The Monthly Status Report shall include the following data elements:

1. Project Name and TO;
2. All work in-progress and completed during the reporting period;
3. Identification of any TO related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals;
4. Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution;
5. Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation;
6. Work planned for the subsequent two reporting periods, when applicable;
7. Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided, each Monthly Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract

These reports shall not be the only means of communication between the Contractor, COR, and the VA Program/Project Manager to advise of performance/schedule issues and to develop strategies for addressing the issues. The Contractor shall continuously monitor performance and report any deviation from the CPMP or previous Bi-Weekly EPMO Status Report to the COR and VA Program/Project Manager during routine, regular communications.

Deliverable:

A. Monthly Status Report

5.1.3 PRIVACY & HIPAA TRAINING

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

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the task.

Deliverables:

A. TMS Training Certificates
B. Signed Contractor Rules of Behavior

5.1.4 TECHNICAL KICKOFF MEETING

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (in-person preferred but can be virtual), agenda (shall be provided to all attendees at least five calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the CO, Contract Specialist, COR, and the VA PgM / PMs.

The Contractor shall deliver the kick-off meeting package three days after the kickoff meeting. The package shall include a work planning and delivery approach, milestone schedule, and constraints.

5.2 VA.GOV CONTENT API

The contractor will support DSVA/DEPO in the creation of new VFS content and tools and the migration from the legacy TeamSite CMS to the modern cloud-based Drupal Content-API. The contractor will be expected to maintain the Content API including the Drupal application, global authoring experience, workflows, content models, user management, and helpdesk support. Specifically, the Contractor shall:

- Operate and maintain the Drupal application and the GraphQL API
- Administer the Drupal system for the VA Drupal community
- Support VA.gov application and platform teams by integrating new and existing web pages and applications into the Global content model

5.2.1 OPERATE, MAINTAIN, AND IMPROVE THE DRUPAL CONTENT API

The Contractor shall operate, maintain, and improve the existing Drupal Content API that delivers content to VA.gov. This includes keeping the application up-to-date, secure, well-

documented, and functional for developers and the authoring community. The contractor will provide regular improvement to the authoring experience, administrative user interface, and application features including custom development, integration, and configuration of third-party modules. The Contractor will support other VA Product Teams creating content pages or web applications on VA.gov by making improvements to the content model, creating or modifying content types, and expanding the functionality of the Drupal application.

Technical documentation for the Content API is available publicly on GitHub: https://github.com/department-of-veterans-affairs/va.gov-cms/blob/master/README.md

5.2.1.1 CONTENT API

The Contractor shall collaborate with the VSP on infrastructure and networking aspects of the Content API. The Content API is part of a larger ecosystem and continuous coordination with the VSP team will be needed to respond to incidents, improve the application, and meet DevOps needs.

The scope of operating and maintaining the Content API for this PWS includes:

- Development and testing of content API (GraphQL) features and enhancements
- Drupal development and testing for global VA.Gov features and third party integrations (e.g. Gov Delivery email API)
- Run and document required VA security scans and perform all required remediation and updates
- Maintain CI/CD pipeline, including a framework for pre-production review instances (currently DevShop), in collaboration with the VSP team
- Maintain the Drupal CMS and GraphQL Github repository and documentation
- Provide documentation and support to VSP team during ATO documentation projects and reviews
- Instrument and monitor the content API to assess performance and alert developers to performance issues and outages
- Respond to incidents in real-time and prepare postmortem reports

5.2.1.2 RELATIONSHIP TO VSP

The Drupal Content API is integrated and depends upon the VSP. The Contractor must coordinate closely with the VSP team to maintain the Content API's VSP integrations and dependencies but will not be held accountable for VSP-owned assets and/or processes. Specifically, the following VSP owned assets and processes are not in scope for this PWS:

- VA Enterprise Cloud infrastructure and networking resources, including code-based definitions and processes
- VA.gov continuous integration and continuous deployment pipeline for pre-production and production environments, including static site build processes
- VA.gov ATO compliance activities, which includes the Content API

- VA.gov developer tools, including automation, monitoring, and incident response tool chains
- Developer access to pre-production and production environments
- Any GitHub repositories associated with the above items
- Any documentation associated with the above items

5.2.1.3 AUTHORING EXPERIENCE

The Contractor shall maintain and improve the global authoring experience provided to VA.gov authors in Drupal. The Contractor shall be responsible for all author-facing experiences, including but not limited to administrative screens (e.g. login), dashboards, the preview experience, and node display. Improvements to the Drupal authoring experience will be based on best practices and features developed in the Drupal community. All solutions will be tested with users in accordance with the Working Principles listed in Section 2 (above). Example tasks include:

- Authoring experience improvements on content management screens specific to individual content types, nodes, or web products
- Development of global features applicable to multiple Drupal authoring groups or products
- Development of new editorial features and dashboards to improve the visual and functional Authoring experience
- Creating Drupal-based reporting functionality for editors and business stakeholders

5.2.1.4 GLOBAL CONTENT MODEL

The Contractor shall maintain the global content model in Drupal and provide support for content governance in the CMS. The Contractor shall support teams developing new pages, tools, and content on VA.gov. Drupal is integral to the creation and maintenance of VA.gov, the contractor will coordinate with teams creating new features and making updates to existing content to ensure the content model reflects the product's needs and use cases. The Contractor will be responsible for communicating with these teams to inform design decision making, implementation of new or existing content design patterns and ensuring best practices are followed in implementing structured content and Search Engine Optimization. This team will support the implementation of new or updated products including providing revisions to global content types and management of re-usable content. Example tasks include:

- Reviewing all third-party contributing CMS and GraphQL code for quality and architectural consistency
- Reviewing all third-party contributing content model updates for consistency, scalability, and to identify gaps in the content model
- Continuously updating the Drupal content model to support any new required content types
- Maintaining content model documentation

5.2.2 SUPPORT THE AUTHORING COMMUNITY

The Contractor shall provide user management, helpdesk, training, and documentation to support the VA.gov authoring community. The current Drupal authoring community at VA is limited to the products described in the Background section, about 40 authors. This community is anticipated to grow into the hundreds within the PoP of this PWS with an anticipated maximum size of 1000 authors. Support activities include but are not limited to:

- Administering Content API access and governance including provisioning accounts, assigning users roles, and managing permissions
- Providing author training and maintain training documentation
- Providing Tiers 1, 2, and 3 helpdesk response, triage and support for issues specific to the Drupal Content API during normal national operating hours (8am – 8pm EST)
- Maintaining the relationship with the VA Enterprise Service Desk (ESD) and knowledge management articles
- Monitoring existing support and admin email boxes and respond to messages
- Supporting editors during migration and content entry projects
- Researching, designing, and developing workflows for VA user management and permission requests

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 VA TECHNICAL REFERENCE MODEL

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

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

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

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

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

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

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

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

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/transition-to-ipv6.pdf). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-267.pdf), the Technical Infrastructure for USGv6 Adoption (https://www.nist.gov/programs-projects/usgv6-program), and the NIST SP 800 series applicable compliance (https://csrc.nist.gov/publications/sp) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

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

6.1.5 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Office 365 ProPlus. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Windows 10. However, Windows 10 is not the VA standard yet and is currently approved for limited use during its rollout. We are in-process of this rollout and making Windows 10 the standard for OI&T. Upon the release approval of Windows 10 as the VA standard, Windows 10 will supersede Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package with switches for silent and unattended

installation and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.6 AUTHORITATIVE DATA SOURCES

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

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

6.2 SECURITY AND PRIVACY REQUIREMENTS

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

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☒	☐	☐
5.2	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.

b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.

d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:

    1) Optional Form 306

2) Self-Certification of Continuous Service
3) VA Form 0710
4) Completed SIC Fingerprint Request Form

e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed "Contractor Rules of Behavior", and with a valid, operational PIV credential for PIV-only logical access to VA's network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
k. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010,

MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

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

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

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

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

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

6.6 GOVERNMENT FURNISHED PROPERTY

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

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

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

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

1. **4** laptops

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

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

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

6.7 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this PWS, the Contractor shall comply with the following Applicable Documents:

1. "Federal Information Security Modernization Act of 2014"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
4. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
5. FIPS Pub 2012, "Personal Identity Verification of Federal Employees and Contractors," August 2013
6. VA Directive and Handbook 6102, "Internet/Intranet Services," July15, 2008
7. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
8. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
9. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
10. 10.VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
11. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
12. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
13. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
14. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
15. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
16. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
17. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
18. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
19. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
20. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

21. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
22. Experience with incorporating and using open source technologies (https://sourcecode.cio.gov/OSS/).
23. The Agile Manifesto (http://www.agilemanifesto.org/)
24. The U.S. Digital Services Playbook (https://playbook.cio.gov/)

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS) 2.0, and will be tracked therein. The TMS 2.0 may be accessed at https://www.tms.va.gov/SecureAuth35/
. If you do not have a TMS 2.0 profile, go to

https://www.tms.va.gov/SecureAuth35/
and click on the "Create New User" link on the TMS 2.0 to gain access.

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

A2.0 VA Enterprise Architecture Compliance

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

A2.1. VA Internet and Intranet Standards

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

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

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

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

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

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

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

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

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

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

A3.2. Compatibility with Assistive Technology

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

A3.3. Acceptance and Acceptance Testing

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

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

A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.

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

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained

during the performance this contract, the Contractor has a responsibility to ask the VA CO.

5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 OEM HARDWARE REQUIREMENTS

The Contractor shall ensure that information technology products are procured and/or services are performed with products that are new equipment and new parts for the required services described herein; no used, refurbished, or remanufactured equipment or parts shall be provided under any circumstances. Absolutely no “Gray Market Goods” or “Counterfeit Electronic Parts” shall be provided. Gray market goods are defined as genuine branded goods intentionally or

unintentionally sold outside of an authorized sales-territory or by non-authorized dealers in an authorized territory. All equipment shall be accompanied by the original equipment manufacturer's (OEM's) warranty. Counterfeit electronic parts are defined as unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

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

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor

or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

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

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

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

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

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

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

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

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

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*

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

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

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

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

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

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

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

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

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

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

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

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

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** based on the severity of the incident.

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

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

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

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

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

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

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

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

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

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

1) Vendor must accept the system without the drive;

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

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

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

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

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to

patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

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

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

d. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The Contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

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

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

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

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:

a) date of occurrence;

b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;

3) Number of individuals affected or potentially affected;

4) Names of individuals or groups affected or potentially affected;

5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;

6) Amount of time the data has been out of VA control;

7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);

8) Known misuses of data containing sensitive personal information, if any;

9) Assessment of the potential harm to the affected individuals;

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and

11) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

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

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

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

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

1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior, relating to access to VA information and information systems;

2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176) and complete this required privacy and information security training annually;

3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

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

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

SECTION C - CONTRACT CLAUSES

C.1 FSS RFQ INTRODUCTORY LANGUAGE

The terms and conditions of the contractor's FSS contract (including any contract modifications) apply to all Blanket Purchase Agreements (BPA) and task or delivery orders issued under the contract as a result of this RFQ. When a lower price has been established, or when the delivery terms, FOB terms, or ordering requirements have been modified by the BPA or task/delivery order, those modified terms will apply to all purchases made pursuant to it and take precedence over the FSS contract. Any unique terms and conditions of a BPA or order issued under the contract that are not a part of the applicable FSS contract will govern. In the event of an inconsistency between the terms and conditions of a BPA or task/delivery order and the Contractor's FSS terms, other than those identified above, the terms of the FSS contract will take precedence.

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

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

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

(End of Clause)

FAR Number	Title	Date
52.203-3	GRATUITIES	APR 1984
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS	JAN 2017
52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES	JUL 2018
52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE EQUIPMENT	AUG 2019
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS	OCT 2018
52.212-4	CONTRACT TERMS AND CONDITIONS—COMMERCIAL ITEMS ALTERNATE I	JAN 2017
52.219-6	NOTICE OF TOTAL SMALL BUSINESS SET-ASIDE	NOV 2011
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-14	RIGHTS IN DATA-GENERAL	MAY 2014
52.227-16	ADDITIONAL DATA REQUIREMENTS	JUN 1987
52.245-1	GOVERNMENT PROPERTY	JAN 2017

52.245-1	GOVERNMENT PROPERTY ALTERNATE I	APR 2012
52.245-9	USE AND CHARGES	APR 2012

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

(a) The Government may extend the term of this contract by written notice to the Contractor at any time during the period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 14 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 24 months.

(End of Clause)

C.4 52.219-14 LIMITATIONS ON SUBCONTRACTING (DEVIATION 2019-01)

(a) This clause does not apply to the unrestricted portion of a partial set-aside.

(b) *Definition.* As used in this clause—

"Similarly situated entity" means a first-tier subcontractor, including an independent contractor, that has the same small business program status as that which qualified the prime contractor for the award, and that is considered small for the NAICS code the prime contractor assigned to the subcontract the subcontractor will perform. An example of a similarly situated entity is a first-tier subcontractor that is a HUBZone small business concern for a HUBZone set-aside or sole source award under the HUBZone Program.

(c) *Applicability.* This clause applies only to—

(1) Contracts that have been set aside or reserved any of the small business concerns identified in 19.000(a)(3);

(2) Part or parts of a multiple-award contract that have been set aside for any of the small business concerns identified in 19.000(a)(3);

(3) Contracts that have been awarded on a sole-source basis in accordance with subparts 19.8, 19.13, 19.14, and 19.15; and

(4) Orders set aside for any of the small business concerns identified in 19.000(a)(3) under multiple-award contracts as described in 8.405-5 and 16.505(b)(2)(i)(F).

(d) *Independent contractors*. An independent contractor shall be considered a subcontractor.

(e) *Agreement*. By submission of an offer and execution of a contract, the Offeror/Contractor agrees in performance of the contract in the case of a contract for—

(1) Services (except construction), it will not pay more than 50 percent of the amount paid by the Government for contract performance to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;

(2) Supplies (other than procurement from a nonmanufacturer of such supplies), it will not pay more than 50 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 50 percent subcontract amount that cannot be exceeded;

(3) General construction, it will not pay more than 85 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 85 percent subcontract amount that cannot be exceeded; or

(4) Construction by special trade contractors, it will not pay more than 75 percent of the amount paid by the Government for contract performance, excluding the cost of materials, to subcontractors that are not similarly situated entities. Any work that a similarly situated entity further subcontracts will count toward the 75 percent subcontract amount that cannot be exceeded.

(f) A joint venture agrees that, in the performance of the contract, the applicable percentage specified in paragraph (e) of this clause will be performed by the aggregate of the joint venture participants.

(End of Clause)

C.5 52.227-19 COMMERCIAL COMPUTER SOFTWARE LICENSE (DEC 2007)

(a) Notwithstanding any contrary provisions contained in the Contractor's standard commercial license or lease agreement, the Contractor agrees that the Government will have the rights that are set forth in paragraph (b) of this clause to use, duplicate or disclose any commercial computer software delivered under this contract. The terms and provisions of this contract shall comply with Federal laws and the Federal Acquisition Regulation.

(b)(1) The commercial computer software delivered under this contract may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b)(2) of this clause or as expressly stated otherwise in this contract.

(2) The commercial computer software may be—

(i) Used or copied for use with the computer(s) for which it was acquired, including use at any Government installation to which the computer(s) may be transferred;

(ii) Used or copied for use with a backup computer if any computer for which it was acquired is inoperative;

(iii) Reproduced for safekeeping (archives) or backup purposes;

(iv) Modified, adapted, or combined with other computer software, provided that the modified, adapted, or combined portions of the derivative software incorporating any of the delivered, commercial computer software shall be subject to same restrictions set forth in this contract;

(v) Disclosed to and reproduced for use by support service Contractors or their subcontractors, subject to the same restrictions set forth in this contract; and

(vi) Used or copied for use with a replacement computer.

(3) If the commercial computer software is otherwise available without disclosure restrictions, the Contractor licenses it to the Government without disclosure restrictions.

(c) The Contractor shall affix a notice substantially as follows to any commercial computer software delivered under this contract:

Notice—Notwithstanding any other lease or license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the Government regarding its use, reproduction and disclosure are as set forth in Government Contract No. _____.

(End of Clause)

C.6 VAAR 852.203-70 COMMERCIAL ADVERTISING (MAY 2018)

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

(End of Clause)

C.7 VAAR 852.215-70 SERVICE-DISABLED VETERAN-OWNED AND VETERAN-OWNED SMALL BUSINESS EVALUATION FACTORS (OCT 2019)

(a) In an effort to achieve socioeconomic small business goals, VA shall evaluate offerors based on their service-disabled veteran-owned or veteran-owned small business status and their proposed use of eligible service-disabled veteran-owned small businesses (SDVOSBs) and veteran-owned small businesses (VOSBs) as subcontractors.

(b) Eligible service-disabled veteran-owned small businesses offerors will receive full credit, and offerors qualifying as veteran-owned small businesses will receive partial credit for the Service-Disabled Veteran-Owned and Veteran-Owned Small Business Status evaluation factor.

To receive credit, an offeror must be registered and verified in the Vendor Information Pages (VIP) database.

(c) Non-Veteran offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the VIP database.

(d) Pursuant to 38 U.S.C. 8127(g), any business concern that is determined by VA to have willfully and intentionally misrepresented a company's SDVOSB/VOSB status is subject to debarment for a period of not less than five years. This includes the debarment of all principals in the business.

(End of Clause)

C.8 VAAR 852.215-71 EVALUATION FACTOR COMMITMENTS (OCT 2019)

(a) The offeror agrees, if awarded a contract, to use the service-disabled veteran-owned small businesses (SDVOSBs) or veteran-owned small businesses (VOSBs) proposed as subcontractors in accordance with 852.215–70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors, or to substitute one or more SDVOSBs or VOSBs for subcontract work of the same or similar value.

(b) Pursuant to 38 U.S.C. 8127(g), any business concern that is determined by VA to have willfully and intentionally misrepresented a company's SDVOSB/VOSB status is subject to debarment for a period of not less than five years. This includes the debarment of all principals in the business.

(End of Clause)

C.9 VAAR 852.219-74 LIMITATIONS ON SUBCONTRACTING—MONITORING AND COMPLIANCE (JUL 2018)

(a) This solicitation includes FAR 52.219-6 Notice of Total Small Business Set-Aside (NOV 2011).

(b) Accordingly, any contract resulting from this solicitation is subject to the limitation on subcontracting requirements in 13 CFR 125.6, or the limitations on subcontracting requirements in the FAR clause, as applicable. The Contractor is advised that in performing contract administration functions, the Contracting Officer may use the services of a support contractor(s) retained by VA to assist in assessing the Contractor's compliance with the limitations on subcontracting or percentage of work performance requirements specified in the clause. To that end, the support contractor(s) may require access to Contractor's offices where the Contractor's business records or other proprietary data are retained and to review such business records regarding the Contractor's compliance with this requirement.

(c) All support contractors conducting this review on behalf of VA will be required to sign an "Information Protection and Non-Disclosure and Disclosure of Conflicts of Interest Agreement" to ensure the Contractor's business records or other proprietary data reviewed or obtained in the course of assisting the Contracting Officer in assessing the Contractor for compliance are protected to ensure information or data is not improperly disclosed or other impropriety occurs.

(d) Furthermore, if VA determines any services the support contractor(s) will perform in assessing compliance are advisory and assistance services as defined in FAR 2.101, Definitions, the support contractor(s) must also enter into an agreement with the Contractor to protect proprietary information as required by FAR 9.505-4, Obtaining access to proprietary information, paragraph (b). The Contractor is required to cooperate fully and make available any records as may be required to enable the Contracting Officer to assess the Contractor's compliance with the limitations on subcontracting or percentage of work performance requirement.

(End of Clause)

C.10 VAAR 852.219-75 SUBCONTRACTING COMMITMENTS MONITORING AND COMPLIANCE (JUL 2018)

(a) This solicitation includes the clause: 852.215-70 Service-disabled veteran-owned and veteran-owned small business evaluation factors. Accordingly, any contract resulting from this solicitation will include the clause 852.215-71 Evaluation factor commitments.

(b) The Contractor is advised that in performing contract administration functions, the Contracting Officer may use the services of a support contractor(s) to assist in assessing Contractor compliance with the subcontracting commitments incorporated into the contract. To that end, the support contractor(s) may require access to the Contractor's business records or other proprietary data to review such business records regarding contract compliance with this requirement.

(c) All support contractors conducting this review on behalf of VA will be required to sign an "Information Protection and Non-Disclosure and Disclosure of Conflicts of Interest Agreement" to ensure the Contractor's business records or other proprietary data reviewed or obtained in the course of assisting the Contracting Officer in assessing the Contractor for compliance are protected to ensure information or data is not improperly disclosed or other impropriety occurs.

(d) Furthermore, if VA determines any services the support contractor(s) will perform in assessing compliance are advisory and assistance services as defined in FAR 2.101, Definitions, the support contractor(s) must also enter into an agreement with the Contractor to protect proprietary information as required by FAR 9.505-4, Obtaining access to proprietary information, paragraph (b). The Contractor is required to cooperate fully and make available any records as may be required to enable the Contracting Officer to assess the Contractor compliance with the subcontracting commitments.

(End of Clause)

C.11 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2018)

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

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

(2) *Designated agency* office means the office designated by the purchase order, agreement, or contract to first receive and review invoices. This office can be contractually designated as the receiving entity. This office may be different from the office issuing the payment;

(3) *Electronic form* means an automated system transmitting information electronically according to the accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests;

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

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

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

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

(1) VA's Electronic Invoice Presentment and Payment System at the current website address provided in the contract.

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI).

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

(e) *Exceptions*. If, based on one of the circumstances in this paragraph (e), the Contracting Officer directs that payment requests be made by mail, the Contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for—

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

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

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

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

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

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

D.1 Attachment 0001 - Price Spreadsheet

D.2 Attachment 0002 - Business Associate Agreement

SECTION E - SOLICITATION PROVISIONS

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

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

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

(End of Provision)

FAR Number	Title	Date
52.216-31	TIME-AND-MATERIALS/LABOR-HOUR PROPOSAL REQUIREMENTS-COMMERCIAL ITEM ACQUISITION	FEB 2007
52.217-5	EVALUATION OF OPTIONS	JUL 1990

E.2 52.204-24 REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2019)

As prescribed in 4.2105(a), insert the following provision:

Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2019)

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

Covered telecommunications equipment or services, Critical technology, and Substantial or essential component have the meanings provided in clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Contractors are not prohibited from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(c) Representation. The Offeror represents that--

It [ ] will, [ ] will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation.

(d) Disclosures. If the Offeror has responded affirmatively to the representation in paragraph (c) of this provision, the Offeror shall provide the following information as part of the offer--

(1) All covered telecommunications equipment and services offered (include brand; model number, such as original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(2) Explanation of the proposed use of covered telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b) of this provision;

(3) For services, the entity providing the covered telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known); and

(4) For equipment, the entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

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

The Government contemplates award of a Time and Materials Task Order resulting from this solicitation.

E.4 852.209-70 ORGANIZATIONAL CONFLICTS OF INTEREST (JAN 2008)

(a) It is in the best interest of the Government to avoid situations which might create an organizational conflict of interest or where the offeror's performance of work under the contract may provide the contractor with an unfair competitive advantage. The term "organizational conflict of interest" means that because of other activities or relationships with other persons, a person is unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or the person has an unfair competitive advantage.

(b) The offeror shall provide a statement with its offer which describes, in a concise manner, all relevant facts concerning any past, present, or currently planned interest (financial, contractual, organizational, or otherwise) or actual or potential organizational conflicts of interest relating to

the services to be provided under this solicitation. The offeror shall also provide statements with its offer containing the same information for any consultants and subcontractors identified in its proposal and which will provide services under the solicitation. The offeror may also provide relevant facts that show how its organizational and/or management system or other actions would avoid or mitigate any actual or potential organizational conflicts of interest.

(c) Based on this information and any other information solicited or obtained by the contracting officer, the contracting officer may determine that an organizational conflict of interest exists which would warrant disqualifying the contractor for award of the contract unless the organizational conflict of interest can be mitigated to the contracting officer's satisfaction by negotiating terms and conditions of the contract to that effect. If the conflict of interest cannot be mitigated and if the contracting officer finds that it is in the best interest of the United States to award the contract, the contracting officer shall request a waiver in accordance with FAR 9.503 and 48 CFR 809.503.

(d) Nondisclosure or misrepresentation of actual or potential organizational conflicts of interest at the time of the offer, or arising as a result of a modification to the contract, may result in the termination of the contract at no expense to the Government.

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

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

(1) Include the name, address, fax number, email and telephone number of the protester;

(2) Identify the solicitation and/or contract number;

(3) Include an original signed by the protester or the protester’s representative and at least one copy;

(4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;

(5) Specifically request a ruling of the individual upon whom the protest is served;

(6) State the form of relief requested; and

(7) Provide all information establishing the timeliness of the protest.

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

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

(End of Provision)

E.6 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (JAN 1998)

As an alternative to filing a protest with the contracting officer, an interested party may file a protest with the Deputy Assistant Secretary for Acquisition and Logistics, Risk Management Team, Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420, or for solicitations issued by the Office of Construction and Facilities Management, the Director, Office of Construction and Facilities Management, 810 Vermont Avenue, NW., Washington, DC 20420. The protest will not be considered if the interested party has a protest on the same or similar issues pending with the contracting officer.

(End of Provision)

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

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

(End of Clause)

E.8 BASIS FOR AWARD AND PROPOSAL INSTRUCTIONS

A. BASIS FOR AWARD

Any award will be made based on the best overall (i.e., best value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the four following evaluation Factors: Technical Factor 1 Case Study, Technical Factor 2 Technical Demonstration (TD), Veterans Involvement Factor, and Price. Technical Factor 1 is equally as important as Technical Factor 2, which is significantly more important than Veterans Involvement, which is slightly more important than Price. To receive consideration for award, a rating of no less than “Limited Confidence” must be achieved for Technical Factor 1 and a rating of no less than "Acceptable" must be achieved for Technical Factor 2. The non-Price Factors combined are significantly more important than the Price Factor. Offerors are cautioned that the award may not necessarily be made to the lowest Price offered or the highest rated Technical proposal.

B. FACTORS TO BE EVALUATED

1. TECHNICAL FACTOR 1 – CASE STUDY
2. TECHNICAL FACTOR 2 – TD
3. VETERANS INVOLVEMENT
4. PRICE

C. EVALUATION APPROACH

All proposals shall be subject to evaluation by a team of Government personnel. The Government reserves the right to award without discussions based upon the initial evaluation of proposals. The proposals will be evaluated strictly in accordance with both its written and demonstrated content. Proposals which merely restate the requirement or state that the requirement will be met, without providing supporting rationale, are not sufficient. Offerors who fail to meet the minimum requirements of the solicitation will be rated Unacceptable and/or No Confidence, and thus, ineligible for award.

1. TECHNICAL FACTOR 1 EVALUATION APPROACH - CASE STUDY SUBMISSION. Technical Factor 1 shall evaluate the Government's confidence in the Offeror's ability, as evidenced by the past experience and expertise identified within each Case Study to perform the work required in the Performance Work Statement (PWS).

2. TECHNICAL FACTOR 2 EVALUATION APPROACH - TD. The evaluation of Technical Factor 2 - TD will consider the following:

    a. Understanding of the Problem - Technical Factor 2 will be evaluated to determine the extent to which the Offeror's approach demonstrates a clear understanding of all features involved in solving the problems and meeting and/or exceeding the requirements presented in the solicitation and the extent to which uncertainties are identified and resolutions proposed.

    b. Feasibility of Approach - Technical Factor 2 will be evaluated to determine the extent to which the proposed approach is workable and the end results achievable. It will be evaluated to determine the level of confidence provided the Government with respect to the Offeror's methods and approach in successfully meeting and/or exceeding the requirements in a timely manner.

    The Government may evaluate the Offeror's proposed fully loaded blended labor rates to determine if the proposed rates are unrealistically low in order to assess the ability of the offeror to meet the Performance Work Statement (PWS) requirements and whether the proposal provides the Government with a high level of confidence of successful performance. Unrealistically low fully loaded blended labor rates proposed for a significant quantity of the total labor hours may indicate a high-risk approach to contract performance. This analysis, if undertaken, is for the limited purpose of aiding the agency in measuring the risk of the Offeror's approach to meeting the solicitation requirements. Since the proposed fully loaded blended labor rates are binding, the Government's price evaluation shall not be adjusted as a result of this analysis due to the fact that the Government is not performing a cost realism analysis. However, if the Government deems it necessary to conduct discussions, and as a result of those discussions an Offeror adjusts its labor rates, then those revised fully loaded blended labor rates will also be assessed again under the Price Factor.

3. VETERANS INVOLVEMENT EVALUATION APPROACH.

In accordance with Veterans Affairs Acquisition Regulation (VAAR) 852.215-70 (DEVIATION), Service-Disabled Veteran-Owned and Veteran-Owned Small Business (VOSB) Evaluation

Factors, the Government will assign evaluation credit for an Offeror (prime contractor) which is a Service-Disabled Veteran-Owned Small Business (SDVOSB) or a VOSB. To receive credit, an offeror must be registered and verified in Vendor Information Pages (VIP) database at time of proposal submission and at time of award (https://www.vip.vetbiz.va.gov) and must meet federal small business size standards for the North American Industry Classification System (NAICS) code assigned to this solicitation.

Non-SDVOSB/VOSB Offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation Factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the VetBiz.gov VIP database (https://www.vip.vetbiz.va.gov) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

4. PRICE EVALUATION APPROACH.

Time and Materials: The total evaluated contract price will equal the sum of the total labor price and the total of the Materials/Other Direct Costs (ODC) price (including associated General and Administrative (G&A)/Material Handling Costs) for the entire purchase/task order period, including options, and will be based on the information provided in Attachment 0001 – Price Spreadsheet. The Government will verify the Offeror's calculation of the total proposed price. The Government will adjust the Offeror's proposed Total Evaluated T&M Price if mathematical errors are identified. **The estimated labor hours are for evaluation purposes only and do not obligate the Government to award such labor hours.**

Further, the Offeror shall provide fully loaded blended rates not exceeding those on its GSA Schedule 70 SIN 132 51 Contract. The proposed fully loaded blended T&M labor rates will be used for the prime and all subcontractors/team members in performance of this Task Order and invoicing will be in accordance with paragraph (i) of Alternate I of the clause at Federal Acquisition Regulation 52.212-4 "Contract Terms and Conditions Commercial Items."

All prices shall be rounded to the nearest cent. The Government reserves the right to correct any rounding errors identified in the Offeror's Proposal.

D. PROPOSAL SUBMISSION

Offerors shall be a General Services Administration (GSA) Federal Supply Schedule 70 Contract holder under SIN 132 51 by the Opt-In date, submission due date, and at time of award. All items offered must be on the Offeror's FSS contract by the submission due date for receipt of offers in response to the Request for Quote (RFQ). **Please note, no Contractor Teaming Arrangements or Order Level Materials will be allowed in response to this solicitation.**

An Opt-in shall be provided confirming your intention to take part in this competition no later than 5 PM EST on November 15, 2019 via email to David.Melton@va.gov. Offerors that do not respond affirmatively by the listed date may not participate in the acquisition

and any submitted Proposal will not be evaluated. Proposals shall ONLY be submitted electronically via the GSA eBUY website for GSA Schedule 70 SIN 132 51 no later than the date set forth on the cover page of the solicitation. Any questions regarding the solicitation shall be provided to David.Melton@va.gov no later than 5 PM EST on November 15, 2019.

1. INTRODUCTION

The Offeror's Proposal shall be submitted electronically by the date and time provided on the cover page of the solicitation. The Offeror's proposal shall consist of five (5) volumes. The Volumes are I – Case Study, II – TD, III – Price, IV – Veterans Involvement, and V – Solicitation, Offer & Award Documents, Certifications & Representations. The use of hyperlinks or embedded attachments in proposals is prohibited. Accordingly, any information contained within an embedded attachment and/or hyperlink will neither be accessed nor evaluated.

WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

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

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

All files will be submitted as either a Microsoft Word 2010 (.doc) [if allowing Word documents] 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, printing, 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 the proposal files may be compressed (zipped) into one file entitled "proposal.zip" using WinZip version 6.2 or later version or the proposal files may be submitted individually.

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

Volume Number	Factor	File Name	Page Limitations*
Volume I	Technical Factor 1	Case Study.pdf	6 (3 per Case Study)
Volume II	Technical Factor 2	TD.pdf	5 pages**
Volume III	Price	D.1 Attachment 0001 – Price Spreadsheet	***
Volume IV	Veterans Involvement	VetsI.pdf	None
Volume V	Solicitation, Offer & Award Documents, Certifications & Representations	OfrRep.pdf	None

*A Cover Page, Table of Contents, Cover Letter, 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.

**The Artifacts created during development of this proof of concept, including artifacts from your agile development practices, user-centered design work, and authoring experience implementation, are not included in this page limit.

***Only fill in what is required in Attachment 0001 – Pricing Spreadsheet

(i) VOLUME I - TECHNICAL FACTOR 1 – CASE STUDY:

Offerors shall submit up to two relevant case studies for evaluation. Relevant case studies must demonstrate recent (within the past three-years) performance of tasks detailed in the PWS, related to operating and maintaining a de-coupled Drupal application, administering a Drupal application for a large editor community, and developing the authoring experience and global content model for new products, performed by the Offeror or any proposed subcontractor who will be responsible for at least 30% of your proposed price. Case studies may reflect work completed for Government and/or Commercial clients.

Offerors are strongly encouraged to submit case studies that demonstrate the capability to

perform multiple tasks from the PWS. Case studies may include work performed under any combination of tasks contained in the PWS, but more weight will be given to Offerors whose case studies encompass the greatest number of tasks outlined in the PWS. Offerors are also strongly encouraged to provide case studies that reflect work performed developing and maintaining a de-coupled Drupal application of similar scale to that outlined in the PWS. The Case Studies shall demonstrate an agile methodology and adherence to practices found within the Digital Services Playbook (https://playbook.cio.gov/) and responses shall specifically address how user centered design and user feedback was used during the agile process for developing the authoring experience and defining the content model. Each Case Study submission is limited to three pages in PDF Format.

Offerors must include the following details for each case study submission:

A. Client organization name
B. Period of performance
C. Offeror's role
D. Goals and outcomes, including any metrics produced, identifying how outcomes addressed those goals
E. Technology stack
F. Delivery Methodology, including how user centered design and user feedback were utilized

****Please note if a submitted Case Study(s) relies on the expertise provided by a subcontractor in Technical Factor 1, that the subcontractor(s) shall be included as a proposed subcontractor in each future proposal Volume for this effort including any resultant award. Additionally, should a Case Study of a proposed subcontractor be used in Technical Factor 1, the vendor shall ensure that the vendor clearly accounts for at least 30% of the proposed price in all future Proposal Volumes and the award. Each Offeror's Case Study submission should include a statement clearly confirming that any subcontractor whose experience is used within a Case Study will be utilized for at least 30% of the amount invoiced during performance of the contract. Failure to ensure these conditions may render an Offeror's proposal unacceptable.**

(ii) VOLUME II – TECHNICAL FACTOR 2 – TD

For the TD, the Government will be evaluating the Offerors' ability to develop a user-centered authoring experience within Drupal. The Government will also be evaluating whether the Offeror has the skills required to execute the PWS.

The scenario below details a fictional government problem. The Offeror is required to address the tasks listed below and will be responsible for providing their completed solution in accordance with the instructions detailed below.

Develop a user-centered authoring experience in Drupal
Background

The Veteran Widget Product Office (VWPO) is responsible for managing various digital products that help VA business lines deliver on their missions. Recently, the VWPO conducted discovery on migrating Pension eligibility information from a legacy section of VA.gov to the

modernized VA.gov, which is supported by a de-coupled Drupal application. During discovery, they learned Veterans need the content for Pension eligibility to be available in both English and Spanish languages. The current Drupal application only supports delivering content in one language.

Your team was brought in by the VWPO to develop a solution to this problem. The VWPO has asked you to create a proof-of-concept (in accordance with the Scope/Deliverable paragraph below) for how the Drupal authoring experience for the page: https://www.va.gov/pension/eligibility/ can be modified to accommodate a Spanish version. An example of a previous Spanish language version of this page on the legacy site is https://benefits.va.gov/BENEFITS/espanol/pension_veteran.asp. The content on the legacy Spanish version of the page does not map perfectly to the modernized Pension eligibility page. VWPO does not know how to manage these discrepancies while retaining a satisfying experience of Veteran users.

For your proof of concept, you must create a Drupal-based solution to this problem that will result in a satisfying user experience for both the Veterans viewing the Pension eligibility content on VA.gov and the VA editor community, who need the authoring experience in Drupal to manage this content to be simple, efficient, and easy to learn.

Scope and Deliverables

In response to the scenario above, you will assist VWPO by providing a way for VA Drupal editors to create a Pension eligibility page with content in two languages (English and Spanish). Specifically, your team has been hired to develop a proof of concept solution for the Drupal authoring experience to solve this problem. Your solution must:

- Provide content data for both the English and Spanish versions of pension eligibility via de-coupled Drupal
- Provide a way for the front-end to gain access to the content
- Allow Drupal editors to manage this content in a user-friendly, intuitive way

You must provide access to your proof-of-concept solution via a running Drupal instance with login credentials to validate the solution, also if there is a separate admin login those credentials are also required. **NOTE: Offerors are responsible for providing all information, including the URL, the login, and any passwords, (if there are separate author and admin access levels please ensure both are provided) necessary for Government access to the solution.**

In addition to the proof-of-concept solution, you must provide access to the version control repository (**NOTE: Offerors are responsible for providing all information, including the URL, the login, and any passwords necessary for Government access to the repository)** where the solution was developed which shall include (the first bullet below has no page limit, the second two bullets are limited to a total of 5 pages inclusive of both bullets):

  - Artifacts created during development of this proof of concept, including artifacts from your agile development practices, user-centered design work, and authoring experience implementation
  - An overview of your approach to the TD
  - A list of your assumptions, decisions made, tradeoffs considered, and next steps

Notes on Scope:

- Your team is not expected to develop any page templates for the de-coupled front-end of this site. Your solution should be delivered in Drupal, assuming the front-end will be developed by another team.
- Your team is not expected to recreate the page https://www.va.gov/pension/eligibility/ to be identical to the version of this page currently available on va.gov.

Resources

- Pension eligibility information on legacy VA.gov in Spanish language: https://benefits.va.gov/BENEFITS/espanol/pension_veteran.asp
- Pension eligibility information on modernized VA.gov in English language: https://www.va.gov/pension/eligibility/

Please provide all credentials requested as part of the scenario above with your Volume II submission. Any subcontractors utilized during the TD must comprise at least 30% of the total proposed price in the Price Volume (and must be included in the required statement above related to this requirement). Accordingly, the Offerors shall include in their response which proposed subcontractors took part in the response to the TD, if any.

(iii) VOLUME III– PRICE FACTOR

The Offeror is required to complete and submit the Government provided "Price Spreadsheet" found as Attachment 0001 to the Solicitation. Instructions for the Spreadsheet can be found in the Worksheet entitled "Instructions." The Offeror shall input a fully loaded blended labor rate for each labor category that will be valid for the Prime and its subcontractors. Fully loaded labor rates proposed shall be two decimal places. The estimated labor hours are for evaluation purposes only and do not obligate the Government to award such labor hours.

The proposed fully loaded labor rates shall not exceed those set forth in the Offerors GSA Federal Supply Schedule 70 Special Item Number 132-51 Contract. It is the Government's intent to incorporate all proposed fully loaded labor rates into the resultant task order.

Each labor category specified by the Government in the solicitation Attachment 0001 must be addressed (i.e. no unaddressed labor categories). If a Labor Category listed is not on an Offerors GSA FSS 70 SIN 132-51 contract they must provide a similar labor category as specified in the Attachment 0001 Instructions tab.

The Government will provide the Not-to-Exceed Travel amounts for both Travel and Materials in Attachment 0001. Offerors shall fill in their proposed Material and Handling Rate for both Travel and Materials which will calculate a line item price based on the proposed rate applied to the Not-to-Exceed Value included in the line item. The estimated Travel and Materials Ceilings are for evaluation purposes only and does not obligate the Government to award the full Ceilings.

NOTE: Section B is being provided for informational purposes only. There is no requirement to submit Section B and it will not be used for pricing evaluation purposes.

Price Rounding Issue - The Government requires Offerors to propose unit prices and total prices that are two (2) decimal places and requires the unit prices and total prices to be displayed as two (2) decimal places. Ensure that the two (2) digit unit price multiplied by the item quantity equals the two (2) digit total item price (there should be no rounding).

The Offeror is advised that in no instance shall its proposed labor rates(s) exceed the Offeror's GSA Schedule 70 rate(s). No open market items will be accepted. All proposed labor categories and rates shall be clearly mapped back to the Offeror's GSA Schedule 70 price list along with any discounts being applied. The Offeror shall provide a copy of their current GSA Schedule 70 contract. In accordance with FAR 8.405-4 the Government is requesting price reductions of the Offeror's GSA Schedule 70 ceiling rates/prices.

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

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

(iv) VOLUME IV – VETERANS INVOLVMENT FACTOR

(1) For SDVOSBS/VOSBs: In order to receive credit under this Factor, an Offeror shall submit a statement of compliance that it qualifies as a SDVOSB or VOSB in accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors (DEVIATION). Offerors are cautioned that they must be registered and verified in Vendor Information Pages (VIP) database (https://www.vip.vetbiz.va.gov/ and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award.

(2) For Non-SDVOSBs/VOSBs: To receive some consideration under this Factor, an Offeror must state in its proposal the names of SDVOSB(s) and/or VOSB(s) with whom it intends to subcontract, and provide a brief description and the approximate dollar values of the proposed subcontracts. Additionally, proposed SDVOSB/VOSB subcontractors must be registered and verified in VIP database (https://www.vip.vetbiz.va.gov/) in order to receive some consideration under the Veteran's Involvement Factor and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of proposal submission and time of award.

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

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

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

b. Any proposed terms and conditions and/or assumptions upon which the proposal is predicated. Any terms which deviate may render proposal unacceptable. The Government will not be held to any terms and conditions and/or assumptions found in any other Volume and is not responsible for reviewing other Volumes for any terms and conditions and/or assumptions.
c. Offerors shall provide list of all proposed subcontractors including company name, percentage of proposed dollars paid, CAGE code and DUNS number.
d. Offerors shall provide a copy of their GSA Schedule 70 contract including their Labor Rate attachment.