



R3 Telecommunications Business Office, OI&T



DRAFT PERFORMANCE WORK STATEMENT (PWS)

**DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
VHA Region 3 Telecommunications Business Office (TBO)**

**Department of Veterans Affairs Region 3 Pager Services
Date: November 21, 2014
TAC-15-16039
PWS Version Number: 1.9**

Contents

1.0	BACKGROUND.....	3
2.0	APPLICABLE DOCUMENTS	3
3.0	SCOPE OF WORK.....	6
4.0	PERFORMANCE DETAILS.....	7
4.1	CONTRACT TYPE.....	7
4.2	PERFORMANCE PERIOD.....	7
4.3	PLACE OF PERFORMANCE.....	7
4.4	TRAVEL	7
5.0	SPECIFIC TASKS AND DELIVERABLES.....	7
5.1	PROJECT MANAGEMENT.....	7
5.1.1	PROGRAM PROGRESS REVIEWS (BASE CONTRACT LEVEL)	7
5.1.2	TECHNICAL KICKOFF MEETING (TASK ORDER LEVEL).....	8
5.2	PAGER LEASING	8
5.3	PAGER SERVICE REQUIREMENTS	10
5.4	OPTIONAL PAGER SERVICES	10
5.5	PAGING SERVICE CONTRACT TRANSITION (BASE CONTRACT LEVEL) ..	11
5.6	PAGER SERVICE PLANS	12
5.7	PAGER MANAGEMENT SERVICES.....	12
5.7.1	SUBSEQUENT PAGER REPLACEMENT.....	13
5.7.2	RETURNS SHIPPING SUPPORT	13
5.7.3	URGENT DELIVERIES FOR BASE AND OPTION YEARS	13
5.8	WEB-BASED PORTAL (BASE CONTRACT LEVEL)	13
5.8.1	SYSTEM CAPABILITIES.....	13
5.8.2	REPORTS	13
5.8.3	END-USER TRAINING (BASE CONTRACT LEVEL).....	14
5.9	INTEGRATED RESOURCE MANAGEMENT (IRM) SYSTEMS (TASK ORDER LEVEL)	14
6.0	GENERAL REQUIREMENTS	15
6.1	ENTERPRISE AND IT FRAMEWORK.....	15
6.2	POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	16
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S)	17
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS	18
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES	20
6.4	PERFORMANCE METRICS	20
6.5	FACILITY/RESOURCE PROVISIONS.....	21
6.6	GOVERNMENT FURNISHED PROPERTY	21
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED	22
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.....	29

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), is to support the provision of benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' healthcare systems in an effective, timely, and compassionate manner. VA depends on Information Management/Information Technology systems to meet mission goals.

OI&T Region 3 Telecommunications Business Office (TBO) is responsible for providing pager devices and related pager services to VA Medical Centers and responsible outliers throughout Region 3, Veterans Integrated Service Networks (VISN) 6, 7, 8, 9, 10, and 11 which has a nationwide footprint to include but not limited to Puerto Rico, Alabama, Florida, Georgia, Illinois, Indiana, Kentucky, Michigan, North Carolina, Ohio, South Carolina, Tennessee, Virginia, and West Virginia.

The VHA OI&T Region 3 TBO was chartered to centralize management and lower the total cost of ownership of telecommunications in Region 3, particularly in monthly recurring charges.

The purpose of this effort is to establish an Indefinite Delivery Indefinite Quantity (IDIQ) contract for centralized, Contractor-leased pager services for VA Region 3.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, <http://www1.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, <http://www1.va.gov/vapubs/>

Region 3 TBO Pager Services Consolidation
TAC-15-16039

10. VA Directive 6102, "Internet/Intranet Services," July 15, 2008
11. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000
13. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, , 2012
18. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," September 20, 2012
19. VA Handbook 6500.1, "Electronic Media Sanitization," March 22, 2010
20. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)", January 6, 2012
21. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of Va Information Systems," February 3, 2014
22. VA Handbook, 6500.5, "Incorporating Security and Privacy in System Development Lifecycle" March 22, 2010
23. VA Handbook 6500.6, "Contract Security," March 12, 2010
24. Project Management Accountability System (PMAS) portal
(reference <https://www.voa.va.gov/pmas/>)
25. OI&T ProPath Process Methodology
(reference <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27>)
NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference
at <http://www.va.gov/trm/TRMHomePage.asp>)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, "Transition to IPv6", September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014

Region 3 TBO Pager Services Consolidation
TAC-15-16039

34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
36. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))
47. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>))
48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
49. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552>)

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- 52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
- 53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
- 54. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
- 55. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
- 56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
- 57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
- 58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013

3.0 SCOPE OF WORK

The Contractor shall provide necessary hardware and support for VA's pager services. This shall include, but may not be limited to leased pagers of various device types, features, and plans to meet the needs of VA Region 3 described herein. The Contractor leased pager services shall also provide VA personnel with access to a web-based portal for management of moves, adds, and changes. The Contractor shall also provide training, maintenance, shipping, and return support. In addition, the Contractor shall support the maintenance and the installation and/or removal of two-way local pager consoles, transmitters, and related equipment at VHA Region 3 locations.

The Contractor shall provide like-for-like services as compared to what is currently installed at facilities. The Government is not responsible for purchasing any new equipment to accommodate contractor services due to any Contractor inability to provide coverage. The Government intends to utilize a transition period (as required) to ensure service continuity. The Contractor shall ensure that all pager services provided under this contract are eligible for the United States Homeland Security Telecommunications Priority Service (TPS) Restoration program.

The tasks described in this PWS are general requirements that may be required in subsequent task orders. Specific requirements will be defined in the individual task orders to be awarded under this IDIQ contract. Not all requirements described in Section 5.0 will apply to each task order, but those that do apply will be cited and expanded upon in the PWS for each task order.

The Contractor shall provide base contract-level reporting, task order level reporting, project management services, pager leasing services, pager device accessories, pager device service plans, pager management services, a web based portal service, and support and maintain Integrated Resource Management (IRM) Systems.

4.0 PERFORMANCE DETAILS

4.1 CONTRACT TYPE

This is an IDIQ Multiple Award Task Order (TO) Contract. Individual TOs shall be issued on a performance-based Firm-Fixed Price (FFP) basis.

4.2 PERFORMANCE PERIOD

The ordering period for the basic contract shall be 5 years from the date of award.

4.3 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed at Contractor and Government facilities.

4.4 TRAVEL

Travel shall be in accordance with individual task order requirements.

5.0 SPECIFIC TASKS AND DELIVERABLES

5.1 PROJECT MANAGEMENT

5.1.1 PROGRAM PROGRESS REVIEWS (BASE CONTRACT LEVEL)

The Contractor shall conduct Program Progress Reviews (PPR) for Government personnel at a mutually agreeable facility (can be virtual). The Contracting Officer (CO) or the Contracting Officer Representative (COR) will schedule the initial PPR. It is anticipated that the first PPR will occur no later than 90 calendar days after date of contract award. Thereafter, PPRs shall occur quarterly, for the life of the contract. During each PPR, the Contractor shall present material that addresses:

1. Status of task orders
2. Actions under warranty and maintenance
3. Significant trends in usage of data, voice, and devices
4. Activities determined to be of importance to VA, such as unanticipated problems and high visibility issues identified by VA
5. Status of significant program events
6. Coverage issues and resolutions, to include outages

The Contractor shall produce and distribute the PPR meeting minutes identifying the key discussion points and action items. The Contractor shall deliver the presentation materials and PPR meeting minutes to the CO and COR within five days after the PPR briefing.

Deliverables:

- A. PPR Presentation Materials

Region 3 TBO Pager Services Consolidation
TAC-15-16039

B. PPR Meeting Minutes

5.1.2 TECHNICAL KICKOFF MEETING (TASK ORDER LEVEL)

The Contractor shall hold a technical kickoff meeting within 10 days after each 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 (can be virtual), agenda (shall be provided to all attendees at least 5 calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within 3 calendar days after the meeting). The Contractor shall invite the CO, Contract Specialist (CS), COR, and the VA Program Manager.

5.2 PAGER LEASING

The Contractor shall provide leased one-way and two-way messaging services, and wireless information services to Region 3, VISN 6, 7, 8, 9, 10, and 11 which includes but is not limited to Puerto Rico, Alabama, Florida, Georgia, Illinois, Indiana, Kentucky, Michigan, North Carolina, Ohio, South Carolina, Tennessee, Virginia, West Virginia. The Contractor shall provide a nation-wide service coverage area that covers the Continental United States and its territories to include Alaska, Hawaii, and Puerto Rico. These services may be offered on a local, statewide, regional, or national basis using digital networks. Such services must be able to address the requirements associated with exclusively provisioned and dedicated to critical messaging paging services. The number of numeric and alphanumeric pagers and services throughout the Period of performance (PoP) is expected to remain relatively static. VA anticipates deviation +/- 5% of the total numbers and types of these pagers in each option year from the prior year, due to the fluidity of employee numbers and needs. Two-way paging and waiting area paging is seeing relative increase due to customer service initiatives. It is anticipated that the need for these pagers may increase by 5% per year.

The Contractor shall provide paging services described herein for any of the sites below. This is provided for informational purposes only. Additional sites may be included in TOs as the requirement for pager services coverage changes. The Contractor's standard commercial warranty shall apply to furnished or installed equipment. All pagers shall include standard paging service.

Ann Arbor, MI	Asheville, NC	Atlanta, GA	Augusta, GA
Battle Creek, MI	Bay Pines, FL	Beckley, WV	Birmingham, AL
Charleston, SC	Chillicothe, OH	Cincinnati, OH	Cleveland, OH
Columbia, SC	Columbus, OH	Danville, IL	Dayton, OH
Detroit, MI	Dublin, GA	Durham, NC	Fort Wayne, IN
Gainesville, FL	Hampton, VA	Huntington, WV	Indianapolis, IN
Lexington, KY (Cooper's)	Lexington, KY (Leestown)	Louisville, KY	Marion, IN
Memphis, TN	Miami, FL	Mountain Home, TN	Nashville, TN

Region 3 TBO Pager Services Consolidation
TAC-15-16039

Orlando, FL	Richmond, VA	Saginaw, MI	Salem, VA
Salisbury, NC	Tampa, FL	Tuscaloosa, AL	West Palm Beach, FL

Through the issuance of subsequent TOs, Contractors shall provide the following approximate quantity of leased pagers. This table is for informational purposes only. Quantities and locations may vary:

Site	Numeric Local.	Numeric Regional	Numeric Nationwide	Alpha Local.	Alpha State Wide	Alpha Regional.	Alpha Nation Wide	Two Way	Waiting Area	Site Total
Ann Arbor, MI	186	2	0	60	0	0	0	0	0	248
Asheville, NC	216	0	0	0	0	0	0	0	0	216
Atlanta, GA	7	2	2	438	0	104	3	3	0	559
Augusta, GA	29	227	0	10	0	21	0	0	0	287
Battle Creek, MI	354	0	0	1	0	0	0	0	0	355
Bay Pines, FL	1175	0	0	3	0	0	0	0	0	1178
Beckley, WV	23	0	0	0	0	0	0	0	0	23
Birmingham, AL	0	0	0	57	0	0	0	0	0	57
Charleston, SC	73	5	2	4	0	0	0	0	0	84
Chillicothe, OH	228	0	0	0	0	0	0	0	0	228
Cincinnati, OH	325	0	0	0	0	0	0	0	0	325
Cleveland, OH	0	0	0	1045	0	1	1	0	0	1047
Columbia, SC	134	24	0	10	0	0	2	3	0	173
Columbus, OH	13	0	0	0	0	0	0	0	0	13
Danville, IL	22	1	0	8	0	0	0	0	0	31
Dayton, OH	105	0	0	9	0	0	0	0	0	114
Detroit, MI	339	0	0	6	0	0	0	4	0	349
Dublin, GA	73	0	0	5	0	0	0	0	0	78
Durham, NC	350	0	0	0	0	0	0	0	0	350
Fort Wayne, IN	123	0	0	6	0	0	0	0	0	129
Gainesville, FL	0	0	0	273	0	0	0	0	0	273
Hampton, VA	13	0	0	311	0	0	0	0	0	324
Huntington, WV	0	2	0	0	0	10	0	0	0	12
Indianapolis, IN	11	0	0	1106	0	0	0	0	0	1117
Lexington, KY (Cooper's)	28	0	0	0	0	0	0	0	0	28
Lexington, KY (Leestown)	0	0	0	12	0	0	0	0	0	12

Region 3 TBO Pager Services Consolidation TAC-15-16039

Louisville, KY	431	0	0	12	0	0	0	0	0	443
Marion, IN	0	0	0	0	0	0	0	0	370	370
Memphis, TN	0	0	0	62	0	0	0	0	0	62
Miami, FL	466	0	0	141	0	0	4	3	140	754
Mountain Home, TN	15	0	0	30	0	0	0	0	0	45
Nashville, TN	0	0	0	621	8	0	0	0	0	629
Orlando , FL	33	0	0	474	0	0	0	0	0	507
Richmond, VA	1319	6	1	40	0	1	0	10	99	1476
Saginaw, MI	52	0	1	17	8	0	1	0	0	79
Salem, VA	0	0	0	0	0	0	0	30	0	30
Salisbury, NC	406	0	0	292	0	0	0	0	0	698
Tampa, FL	945	2	0	173	0	0	0	10	0	1130
Tuscaloosa, AL	61	0	0	1	0	0	0	0	0	62
West Palm Beach, FL	397	0	0	60	0	0	0	3	0	460
Lease Total	7952	271	6	5287	16	137	11	66	609	14355

5.3 PAGER SERVICE REQUIREMENTS

Standard Paging Services
<p>A. Numeric Paging Users transmit and receive numeric messages or codes.</p>
<p>B. 2-Way Paging Users have the capability to either receive or send text messages to another two-way device, email address, or text-enabled mobile phone.</p>
<p>C. Alphanumeric Paging Users transmit and receive either alphabetic and numeric messages or codes.</p>

5.4 OPTIONAL PAGER SERVICES

Occasionally, the Government will require a given pager to have optional features/services. Typical additional features/services include numeric retrieval, call forwarding, voicemail, group call/follow, alias, etc. See below for a non-comprehensive list of additional features/services.

Optional Paging Services

Region 3 TBO Pager Services Consolidation
TAC-15-16039

A. Waiting area Paging Users receive alert-only paging with any combination of beep, vibrate, and LED flash notification.
B. Send a specific message to a mass audience during an emergency or when a large number of people need to be notified of a common message.
C. Copy incoming pages to an unlimited number of addresses including pager, cellular, and email.
D. Send messages to alphanumeric or two-way pager using an easy-to-remember alias address.
E. Secondary number assignment for devices including local and toll-free service.
F. Text or numeric message distributed to a pre-established group of pagers.
G. Two-way device can communicate directly with any SMS-equipped phone.
H. Two-Way Group Call Feature.
I. Message sent to pager can be copied to addresses or devices such as email and SMS.
J. Message carbon copy.
K. Displays critical messages on any PC, tablet or smartphone in an application.
L. 24/7 live operator answered dispatch service that will send alphanumeric messages to the pager owner.
M. Personalized greeting for callers to hear.
N. Message delivery services to ensure pages are not missed if the pager is left at home, leaves the coverage area, or if the battery runs down.
O. Forward your page/message to another pager or to any email address.
P. Allow end-users to call their own pager numbers to retrieve numeric pages.
Q. Personal greeting.
R. Private voice mailbox.
S. Send messages from a personal computer to a pager.
T. Simultaneous transmission of pager number to the assigned pager and additional numbers, such as a cell, smart phone whether a single device or group.
U. Multi-Messenger Groups.
V. Clinical alerting and notification.

5.5 PAGING SERVICE CONTRACT TRANSITION (BASE CONTRACT LEVEL)

In the event of a change in pager service provider, the Contractor shall ensure there are no service disruptions during the transition of one service provider to another. In addition, the Contractor shall ensure that the configuration of existing services is maintained (e.g. pager groups, features). The Contractor shall port 100% of all original pager numbers. The Contractor shall identify all current business processes which are dependent on the paging system and have those business processes configured and activated to prevent service disruption as well. Examples of business processes include group paging, reaction team paging and email alerting. The Contractor shall document the detailed transition steps in a Paging Services Transition Plan which shall be

Region 3 TBO Pager Services Consolidation
TAC-15-16039

reviewed and approved by the Government. In the event lower than the coverage defined in each task order is provided, the Contractor shall be responsible for any remedy needed to provide adequate coverage including but not limited to the installation of an additional transmitter or antenna. Service coverage issues shall be remediated within 30 days of being identified by the Government. Specific requirements will be defined in the individual task orders to be awarded under this IDIQ contract.

5.6 PAGER SERVICE PLANS

The Contractor shall offer the following service plans:

- a. Unlimited Calls: Numeric, Alphanumeric
- b. Unlimited Characters: Two-Way
- c. Unlimited Service Courtesy Pagers

The Contractor shall notify the VA COR, or his designate, and the VA National Service Desk (NSD) of any scheduled system outages at least 72 hours in advance of the planned outage. In case of any unforeseen outages, the VA-COR and the NSD shall be notified within four hours by both email and telephone call and kept up-to-date on the progress until service restoration. If the unscheduled outage is anticipated to be more than 24 hours, the Contractor shall provide an alternate plan for service coverage acceptable to VA.

These pager services are critical to VA's mission and directly impact VA's ability to provide quality care to our Veterans. The Contractor shall ensure that all pager service plans provided under this contract are eligible for the United States Homeland Security TPS Restoration program. All pager services supplied under this contract must receive priority treatment under the TPS program. In order to facilitate priority services, the Contractor shall ensure that the VA is the officially registered customer with each service provider. The Contractor shall include basic service plans in the cost of the lease for each pager. All VA accounts shall be identified in the Contractor's network as a Federal Government account and shall not be subject to disconnect for any reason other than instances where the Government requests that it be disconnected.

5.7 PAGER MANAGEMENT SERVICES

Contractors shall coordinate initial deliveries with Site Point of Contracts (POC) before shipment of hardware to ensure sites have adequate storage space.

All shipments, either single or multiple container deliveries, shall bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number will indicate total number of containers for the complete shipment (e.g., Package 1 of 2), clearly readable on manifests and external shipping labels.

5.7.1 SUBSEQUENT PAGER REPLACEMENT

The Contractor shall support the replacement of any pager types, including the associated features and plans specified in this PWS.

5.7.2 RETURNS SHIPPING SUPPORT

The Contractor shall supply VA with postage paid Return Shipping Labels for return of unneeded or repairable devices. VA anticipates that 5% of pagers will be returned to be repaired or replaced. In addition, VA may return pagers if VA does not need the pagers to stay within the 3% of spare devices; or, for the purpose of receiving credit for returning unneeded pagers. Include all estimated postage costs in your fixed price line items for shipping and return support. These costs will not be directly reimbursed by the Government.

Prior to shipping, the Contractor shall notify Site POCs, by phone, followed by email, of all incoming deliveries including line-by-line details for review of requirements. The Contractor shall not make any changes to the delivery schedule at the request of the Site POCs. Any changes to the delivery schedule need to be authorized by the COR.

5.7.3 URGENT DELIVERIES FOR BASE AND OPTION YEARS

VA shall contact the Contractor for the purpose of obtaining accelerated delivery for pagers and/or transmitters (e.g., replace a transmitter or antenna in the event of a hurricane). The Contractor shall reply to the inquiry within twenty-four (24) hours after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the VA, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

5.8 WEB-BASED PORTAL (BASE CONTRACT LEVEL)

5.8.1 SYSTEM CAPABILITIES

The Contractor shall provide a web-based access for accounts access and management purposes. It shall also enable facility managers to assign, activate, swap, or disconnect devices in the most expeditious and convenient manner. The VA COR will provide the Contractor with a list of individuals who will need access to the web-based portal and the account numbers.

5.8.2 REPORTS

The Contractor shall provide the VA with the capability of running reports through a web-based portal. The number and names of the individuals will be determined at contract award; not to exceed 50 users. At a minimum, Region 3 TBO, or it's designates, shall be able to access/parse reporting for the following:

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- a. Units in service, by type, billed customer, department.
- b. Calls, by billed customer, pager number, department
- c. Overcalls by billed customer, pager number, department
- d. New sales, charges, or disconnects
- e. Account Summary by sub-accounts
- f. Zero-use devices

5.8.3 END-USER TRAINING (BASE CONTRACT LEVEL)

The Contractor provided web-based portal shall have self-paced web-based help tutorials covering all portal functionality.

In addition, the Contractor shall provide web-based training, such as Live Meeting / Lync, for new VA managers or when significant changes to the web-based content have occurred. Contractor training of VA personnel has historically occurred on a quarterly basis or when need/number is established by VA and coordinated with Contractor. The Contractor shall make any slides used during a live meeting training session available to the trainees.

5.9 INTEGRATED RESOURCE MANAGEMENT (IRM) SYSTEMS (TASK ORDER LEVEL)

VA may require IRM Transmitter installations at VA locations within Region 3.

The Contractor shall provide VA with a draft IRM and Transmitter Proposal for review and approval by the Government. The Contractor proposal shall include an installation schedule, installation process, specify how the system has been designed to support all VA pager needs (e.g., quantities, services) including the growth of pagers anticipated in any following option years. The Contractor shall incorporate all agreed upon updates to the proposal based on VA provided comments within 10 days of the VA and the Contractor reaching an update agreement on all comments.

The Contractor shall install the system according to the installation schedule and plan. The Contractor shall test the system with a Government witness present as per the test plan within 10 days of the system being installed. All test results shall be recorded in a Test Result Report. The report shall include a remediation plan for all observed test failures. The Contractor shall address any test failures, retest to demonstrate that the failures have been remediated, and record the successful testing in a revised Test Result Report.

The Contractor shall furnish all Operating and Maintenance Manuals which are normally provided with the equipment being installed.

The Contractor's standard commercial warranty shall apply to the installed equipment.

This task can be invoked multiple times throughout the period of performance (i.e., base and all option periods).

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), <http://www.ea.oit.va.gov/EAOT/OneVA/EAETA.asp>, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf>), M-05-24 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf>), M-11-11 (<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>) & (<http://www.cybertelecom.org/dns/ipv6usg.htm>). IPv6 technology, in

Region 3 TBO Pager Services Consolidation
TAC-15-16039

accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>) and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (http://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2%200_2013.pdf).

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Region 3 TBO Pager Services Consolidation
TAC-15-16039

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	Background Investigation (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	Tier 1 / National Agency Check with Written Inquiries (NACI) A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	Tier 2 / Moderate Background Investigation (MBI) A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	Tier 4 / Background Investigation (BI) A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
<u>Task Number</u>	<u>Tier1 / Low / NACI</u>	<u>Tier 2 / Moderate / MBI</u>	<u>Tier 4 / High / BI</u>
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Region 3 TBO Pager Services Consolidation
TAC-15-16039

5.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. The Contractor shall bear the expense of obtaining background investigations.
- c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
- e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
 - 1) For a Tier 1/Low Risk designation:
 - a) OF-306
 - b) DVA Memorandum – Electronic Fingerprints
 - 2) For Tier 2/Moderate or Tier 4/High Risk designation:

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- a) OF-306
- b) VA Form 0710
- c) DVA Memorandum – Electronic Fingerprints
- f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
- g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).
- h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
- i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
- j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
- k. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
- l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

- A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

Performance Objective	Performance Standard	Acceptable Performance Levels
A. Technical Needs	<ol style="list-style-type: none">1. Shows understanding of requirements2. Efficient and effective in meeting requirements3. Meets technical needs and mission requirements4. Offers quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none">1. Quick response capability2. Products completed, reviewed, delivered in timely manner3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Project Staffing	<ol style="list-style-type: none">1. Currency of expertise2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Value Added	<ol style="list-style-type: none">1. Provided valuable service to Government2. Services/products delivered were of desired quality	Satisfactory or higher

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

6.5 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 will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements (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

Not applicable.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

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

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

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

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

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

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at <http://www.ea.oit.va.gov/index.asp> in force at the time of issuance of this contract, including the Program Management Plan

and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

A2.1. VA Internet and Intranet Standards:

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

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

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

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

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

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

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

- ☒ § 1194.21 Software applications and operating systems
- ☒ § 1194.22 Web-based intranet and internet information and applications
- ☒ § 1194.23 Telecommunications products

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- ☒ § 1194.24 Video and multimedia products
- ☒ § 1194.25 Self contained, closed products
- ☒ § 1194.26 Desktop and portable computers
- ☒ § 1194.31 Functional Performance Criteria
- ☒ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

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

A3.4. Representation of Conformance

In order to be considered eligible for award, offerors must submit the Government Product Accessibility Template (GPAT) to verify Section 508 conformance of their products and/or services. The GPAT will be incorporated into the resulting contract.

A3.5. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include a final/updated GPAT and final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for 508 Compliance before delivery. The Contractor shall be able to demonstrate 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at <http://www.section508.va.gov/section508/Resources.asp>.

Deliverable:

- A. Updated GPAT
- B. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

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

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

A5.0 Confidentiality and Non-Disclosure

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

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

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA Contracting Officer will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA Contracting Officer for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
 4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA Contracting Officer.
 5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
 6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
 7. Contractor must adhere to the following:
 - a. The use of "thumb drives" or any other medium for transport of information is expressly prohibited.
 - b. Controlled access to system and security software and documentation.
 - c. Recording, monitoring, and control of passwords and privileges.
 - d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

Region 3 TBO Pager Services Consolidation
TAC-15-16039

- h. Contractor does not require access to classified data.
- 8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
- 9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, "Federal Leadership in Environmental, Energy, and Economic Performance," dated October 5, 2009; Executive Order 13423, "Strengthening Federal Environmental, Energy, and Transportation Management," dated January 24, 2007; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, FEMP designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

- 1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).
- 2. Provide/use the purchasing specifications listed for FEMP designated products at www.femp.energy.gov/procurement. The Contractor shall use the low standby power products specified at <http://energy.gov/eere/femp/low-standby-power-products>.
- 3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

Region 3 TBO Pager Services Consolidation
TAC-15-16039

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

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

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

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

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

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

Not Applicable

B3. VA INFORMATION CUSTODIAL LANGUAGE

Not Applicable

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Not Applicable

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

Not Applicable

B6. SECURITY INCIDENT INVESTIGATION

Not Applicable

B7. LIQUIDATED DAMAGES FOR DATA BREACH

Not Applicable

B8. SECURITY CONTROLS COMPLIANCE TESTING

Not Applicable

B9. TRAINING

Not Applicable