Performance Work Statement (PWS)

for the

Veterans Intake, Conversion and Communications Services (VICCS)

Date: June 14, 2019

Department of Veterans Affairs

Office of Administration and Facilities

Acquisition Division

Version History

Version #	Version Description	Release Date
1.0	Initial Release	April 2019
2.0	Revised for Solicitation	June 2019

Contents

1.0 Scope

Through its three (3) administrations, National Cemetery Administration (NCA), Veterans Benefits Administration (VBA), and Veterans Health Administration (VHA), VA administers vital services to America's veterans. VA provides health care services, benefits programs and access to national cemeteries to former military personnel and their dependents.

The fundamental mission of the Veterans Benefits Administration (VBA) is to provide Veterans, service members, and their families benefits earned through military service to the United States. VBA accomplishes its mission by providing services supporting Veteran readjustment to civilian life and enhancements to their well-being.

VBA developed the Veterans Benefits Management System (VBMS), a paperless claims processing system that enables efficiencies, thereby reducing the time required to process claims for benefits. The system replaces a manual and paper-based process comprised of inherent bottlenecks and inefficiencies.

Populating the VBMS document repository requires ongoing conversion efforts consisting primarily of converting claims-related source materials. Such materials are received in either paper or electronically via fax or other electronic means, or through converting other non-paper source materials. These materials can include: microfilm, microfiche, files stored on Compact Discs (CD), Digital Video Disc / Digital Versatile Disc (DVDs), and flash memory devices. All materials are converted into searchable Portable Document Format (PDF) files, associated metadata is captured, and the images and metadata are uploaded into the VBMS repository.

To continuously improve benefits processing efficiency and cycle-time, VBA has partnered with industry leaders to provide a host of contracted services. Services in the existing contract portfolio include:

- File bank extraction services reduced VBA’s physical footprint at 56 regional offices across the nation, saving taxpayers millions of dollars.
- Conversion services that provide images and metadata to VBMS eFolders.
- Digitized Mail Handling Service (DMHS) that provides a digital preview of converted mail.
- Records Management Services (RMS) that provide storage for converted source materials.
- Centralized Benefits Communications Management (CBCM) services supporting the centralization of printing and mailing for all VA regional offices.
- Services supporting Private Medical Records (PMR) retrieval.

Through these partnerships VBA continues to progress from paper-based processes to an electronic environment supporting greater automation and improved efficiencies. This progression continues through the acquisition of managed services that include the capabilities to:

- Perform intake services

- Perform tracking, handling (including physical storage), and management of all source materials
- Perform conversion services
- Perform inbound and outbound mail management
- Facilitate transaction processing / case management
- Perform centralized outbound services
- Perform data reconciliation and data transfer to VA and other Contractor systems and services
- Develop training and communications materials and facilitate change management where new policies, business rules / procedures, or systems changes are implemented
- Assist VA with development and documentation of business processes, rules, and tools to create and / or improve:
    - Data analytics and business process intelligence
    - Data visualization
    - Inbound / outbound mail processing
    - Document taxonomy management
    - Document processing / editing tools
    - New business rules creation for new business processes
    - Business rules management
    - Training
    - Forms development and modification
- Perform analysis using the developed business processes, rules, and tools

This PWS provides general requirements. Specific requirements shall be defined in individual Task Orders. Service area requirements are described in Section 4.0 and are not mutually exclusive for Task Order requirements. Requirements may fall within one specific service area but in many cases, the requirements will encompass and apply across and within multiple service areas. Service performance requirements shall be established in individual Task Orders.

2.0 Applicable Documents

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

1. 44 U.S.C. § 3551-3558, “Federal Information Security Modernization Act (FISMA) of 2014”

2. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”

3. Federal Information Processing Standards (FIPS) Publication 140-3, “Security Requirements for Cryptographic Modules”

4. FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004

5. FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
6. FIPS Publication 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
7. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
8. Public Law 109-461, “Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters”
9. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, http://www.va.gov/vapubs/
10. VA Handbook 0710, “Personnel Security and Suitability Security Program,” May 2, 2016, http://www.va.gov/vapubs
11. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
12. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards”
13. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
14. 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
15. NIST Special Publication (SP) 800-66 Rev 1: “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” October 2008
16. “Homeland Security Presidential Directive (12) (HSPD-12),” August 27, 2004
17. VA Directive 6500, “VA Cybersecurity Program,” January 23, 2019
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” March 10, 2015
19. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI)”, March 12, 2019
20. VA Handbook 6500.3, “Assessment, Authorization, and Continuous Monitoring of VA Information Systems,” February 3, 2014
21. VA Handbook 6500.5, “Incorporating Security and Privacy in System Development Lifecycle,” March 22, 2010
22. VA Handbook 6500.6, “Contract Security,” March 12, 2010
23. VA Handbook 6500.8, “Information System Contingency Planning,” April 6, 2011

24. “One-VA Technical Reference Model (TRM)” - (reference at https://www.va.gov/trm/TRMHomePage.aspx)
25. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
26. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
27. VA Directive 6510, “VA Identity and Access Management,” January 15, 2016
28. VA Handbook 6510, “VA Identity and Access Management,” January 15, 2016
29. VA Directive 6300, “Records and Information Management,” September 21, 2018
30. VA Handbook, 6300.1, “Records Management Procedures,” March 24, 2010
31. NIST SP 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Rev. 2,” December 20, 2018
32. NIST SP 800-53 Rev. 5 (DRAFT), “Security and Privacy Controls for Federal Information Systems and Organizations,” August 15, 2017
33. OMB Memorandum, “Transition to Internet Protocol version 6 (IPv6),” September 28, 2010
34. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
35. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
36. OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies,” December 16, 2003
37. OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors,” August 5, 2005
38. 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
39. OMB Memorandum for Chief Information Officers, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
40. “Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance,” December 2, 2011

41. NIST SP 800-116 Rev. 1, “Guidelines for the Use of PIV Credentials in Facility Access,” June 29, 2018
42. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” December 1, 2017
43. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 19, 2014
44. “Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication,” March 2014
45. “IAM Identity Management Business Requirements Guidance Document,” May 2013, (https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
46. VA Memorandum, VAIQ #7712300, “Mandate to meet PIV Requirements for New and Existing Systems,” June 30, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846
47. “Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.2, Federal Interagency Technical Reference Architectures, Department of Homeland Security,” June 19, 2017
48. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC),” November 20, 2007
49. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
50. 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)
51. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
52. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
53. Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015
54. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
55. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access”, January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
56. VA Memorandum, VAIQ #7614373, “Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA

IT Systems," July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

57. VA Memorandum, VAIQ #7613595, "Mandatory Use of PIV Multifactor Authentication to VA Information System," June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
58. VA Memorandum, VAIQ #7613597, "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges," June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
59. VA Memorandum, VAIQ #7581492, "Use of Personal Email," April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
60. VA Memorandum VAIQ #7823189, "Updated VA Information Security Rules of Behavior," September 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
61. "Records Control Schedule VB-1," dated January 31, 2014
62. VA Handbook 0730, "Security and Law Enforcement" dated August 11, 2000 (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=93&FType=2)
63. VA Handbook 0730/1, "Security and Law Enforcement" dated August 20, 2004 (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=96&FType=2)
64. VA Handbook 0730/4, "Security and Law Enforcement" dated March 29, 2013 (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=700&FType=2)
65. "Authorization Requirements Standard Operating Procedures, v3.31," dated February 4, 2019
66. VA Memorandum, VAIQ #7660995, "Continuous Diagnostics and Monitoring of all VA Information Systems," dated January 29, 2016

3.0 General Requirements

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

3.1 Contract Type

This is a Multiple Award Indefinite Delivery/Indefinite Quantity (IDIQ) contract.

3.2 Ordering Period

The ordering period for the basic contract shall be five (5) years.

3.3 Hours of Work

Work at a Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). Hours of work will be established at the TO

level. The Contractor may also be required to support 24/7 operations 365 days per year as identified in individual Task Orders.

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

Under current definitions, four are set by date:

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

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

The other six (6) are set by a day of the week and month:

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

3.4 Place of Performance

The place of performance shall be identified in individual Task Orders. Locations will be Government and Contractor sites within the Continental United States (CONUS). No work shall be performed outside of the Continental United States (OCONUS).

3.5 Travel

Travel shall be in accordance with (IAW) individual Task Order requirements. Travel details must be provided to and approved by the Contracting Officer’s Representative (COR) or the Government designee prior to the commencement of travel. All travel shall be IAW FAR 31.205-46.

3.6 Materials, Equipment, and Locations

3.6.1 Government-Furnished

Government Furnished Property (GFP) which includes Government Furnished Material (GFM), Government Furnished Information (GFI), and Government Furnished Equipment (GFE) may be provided and shall be identified in the individual Task Order. The Contractor shall be responsible for conducting all necessary examinations, inspections, maintenance, and tests upon receipt.

VA will provide VA specific system access as appropriate and required in individual Task Orders. Contractors shall comply with VA security policies and procedures with respect to protecting sensitive data. See Section 6.0 for detailed security requirements.

3.6.2 Contractor-Acquired

The Contractor shall acquire and / or provide any hardware and / or software required to accomplish each Task Order that is not provided as GFP. Software integrity shall be maintained by the Contractor within the licensing agreement of the producer.

3.6.3 Connectivity

VA will provide connectivity to VA specific systems / network as required for execution of a task via VA approved remote access technology. Currently this may include but is not limited to Citrix Access Gateway (CAG), site-to-site VPN, or Cisco AnyConnect Secure Mobility Client. The Contractor must meet the requirements of VA Handbook 6500 and will bear the cost to provide connectivity to VA systems / networks. Other connectivity to VA systems may be authorized as appropriate in individual Task Orders.

3.6.4 Facilities

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

3.6.4.1 Government Facilities

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

3.6.4.2 Non-Government Facilities

Personnel shall perform at Contractor facilities as specified in the individual task order and shall comply with VA and/or Federal A&A requirements. The Contractor shall disclose specific facility information during the Request for Task Order Proposal (RTOP) process. All facilities shall be approved by VA and in compliance with PWS paragraph 6.0, Security and Privacy. All facilities containing VA source materials shall be compliant with 36 CFR Part 1234, Subpart B, with no exceptions made for the waivers discussed within 36 CFR Part 1234, Subpart B. While National Archives and Records Administration (NARA) certification is not required, the Contractor shall maintain compliance with the referenced NARA requirements.

3.7 Government Inspection and Oversight

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

a. Provide the CO, COR, and representatives of authorized Government offices, full and free physical and remote / logical access to their facilities, installations, operations documentation, databases, and personnel used for contract hosting services. This access shall be provided to the extent required to carry out audits, inspections, device scanning utilizing Government prescribed tools, investigations, or other reviews to ensure compliance with contractual

requirements for IT and information security, and to safeguard against threats and hazards to the integrity, availability, and confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor).

b. Fully cooperate with all audits, inspections, investigations, or other reviews conducted by or on behalf of the CO or other authorized Government offices as described in subparagraph (a). Full cooperation includes, but is not limited to, prompt disclosure (per agency policy) to authorized requests of data, information, and records requested in connection with any audit, inspection, investigation, or review, making employees of the Contractor available for interview by auditors, inspectors, and investigators upon request, and providing prompt access (per agency policy) to Contractor facilities, systems, data and personnel to the extent the auditors, inspectors, and investigators reasonably believe necessary to complete the audit, inspection, investigation, or other review. The Contractor's (and any Subcontractors') cooperation with audits, inspections, investigations, and reviews shall be provided at no additional cost to the Government.

c. Preserve such data, records, logs and other evidence which are reasonably necessary to conduct a thorough investigation of any computer security incident. A computer security incident (as defined in NIST SP 800-61, Computer Security Incident Handling Guide), includes but is not limited to, those constituting an actual or potential threat or hazard to the integrity, availability, or confidentiality of agency information in the possession or under the control of the Contractor (or Subcontractor), or to the function of information systems operated by the Contractor (or Subcontractor) in the performance of this contract.

d. Promptly notify the designated agency representative in the event of any computer security and privacy incident as described in paragraph (c) above. This notification requirement is in addition to any other notification requirements which may be required by law or this contract. Established Federal agency timeframes for reporting security and privacy incidents to the United States Computer Emergency Readiness Team (US-CERT), although not exhaustive, serve as a useful guideline for determining whether reports under this paragraph are made promptly. (See NIST SP 800-61, Computer Security Incident Handling Guide, Appendix J).

e. Provide to the requestor (CO, a representative of the CO, or authorized Government offices) Government data, information, or records under the control of or in the possession of the Contractor pursuant to this contract, which the Agency or authorized Government offices, including the Office of Inspector General (OIG), may request in furtherance of other audits, inspections, investigations, reviews or litigation in which the Agency or other authorized Government offices are involved in the form specified at the task order level. Requests for production under this paragraph shall specify a deadline not less than 10 days for compliance, which will determine whether response to the request has been made in a timely manner. Unless expressly provided otherwise

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

f. Include the substance of this Section, including this paragraph (f) in any subcontract which would require or otherwise result in Subcontractor employees having access to agency information in the possession or under the control of the Contractor (or Subcontractor), or access to information systems operated by the Contractor (or Subcontractor) in the performance of this contract.

g. Ensure that all hosting services pertaining to this contract are performed within the Continental United States of America, including the storage of agency data, information, and records under the control of or in the possession of the Contractor pursuant to this contract.

3.8 Enterprise and IT Framework

3.8.1 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), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems 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 can 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 if 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.

3.8.2 Authority to Operate (ATO) / Interim Authority to Operate IATO)

The Contractor shall obtain and maintain any ATO or, if acceptable to the Government, any IATO within 180 calendar days following Task Order award. The Contractor shall develop, implement, and execute processes to obtain VA authorizations for all services (including updated services as required) as specified by individual Task Orders. Specific activities include, but are not limited to security certifications, or comprehensive assessments of the management, operational, and technical security controls in Contractor-provided services to determine the extent to which the controls are implemented correctly. For detailed Security and Privacy Requirements refer to Authorization Requirements Standard Operating Procedures Version 3.31.

3.8.3 Browser / Mobile Standards

The Contractor shall ensure services are developed in accordance with VA standard browser baselines and shall update services as required by VA when new browser standards are implemented. In the event mobile services are required, VA mobile development, security and privacy standards should be followed to ensure adequate protection of VA information. VA currently uses Windows IE 11 and anticipates staying with the Windows standard as VA progresses into Windows 10 OS. Although VA has Chrome, it is currently limited in functionality and is not considered the standard browser for daily usage across VA applications.

3.9 Quality Assurance

3.9.1 Quality Assurance Surveillance Plan

In accordance with FAR 37.102, Task Orders issued under this IDIQ will be performance-based to the maximum extent practicable. Each TO will define the quality assurance surveillance plan, to include specific performance standards and measures at the TO level.

3.9.2 Performance Based Service Assessment (PBSA)

The COR shall perform quarterly performance assessments. The Performance Based Service Assessment (PBSA), or other method, may be used to document this assessment. A sample PBSA is provided in this document as Addendum B.

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

3.9.3 Contractor Performance

A Contractor Discrepancy Report (CDR), may be issued by a CO or COR to document less than acceptable performance by the Contractor at any point during the period of performance. It should be noted that issuance of a CDR should not be the first form of communication or plan of resolution unless the seriousness of the situation warrants such formal documentation from onset. The CO, COR and Contractor shall maintain open and effective communications to avoid the issuance of CDRs to the maximum extent practicable. All parties acknowledge that a finalized CDR will become part of the official file and will be used to report on annual performance under the IDIQ. If use of a CDR is warranted, the CO/COR shall complete the CDR, citing the IDIQ and / or TO number and the specific IDIQ and/or TO section or clause related to the performance issue. The CO/COR shall provide a detailed and descriptive narrative of the background and issue. Upon receipt of the CDR, the Contractor shall provide a timely and detailed response. The Contractor's response shall include any important or relevant information or justification for the performance issue and a proposed resolution. The CO/COR will review the response from the Contractor and the CO will issue a final recommendation

or plan of action. The CO, COR, and Contractor will maintain communication to ensure that the recommendation or plan of action is carried out.

The Contractor's performance on the IDIQ and any TOs will be reported to the Contractor Performance Assessment Reporting System (CPARS) on an annual basis. The CO and COR will make use of information from CDRs and the Task Order Performance Evaluations, as well as any additional knowledge and information available to them with respect to the Contractor's performance, to complete the CPARS. Contractors shall familiarize themselves with the CPARS process and be prepared to respond to reports entered by the CO and COR.

3.10 Independent Quality Assurance and Monitoring (QA&M)

The Contractor is responsible for the quality of all work performed. All work performed either by Contractor employees or by Subcontractors shall be subject to quality review. The government will implement an independent, third party QA&M contract.

As described in individual Task Orders, the Contractor may be required to support full-time onsite government QA&M staff and to support activities including but not limited to:

- Making available program, project, and operational documents
- Providing data requested as part of onsite and remote audits
- Providing access to source materials, images and associated metadata
- Complying with sampling methodologies or practices required by the government

Unless otherwise specified, within 30 calendar days of any Task Order award, the VICCS Contractor shall provide any resources necessary to support QA&M as specified in the individual Task Order. These requirements may include making available full-time space at the Contractor's facility.

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

The Contractor shall develop, implement, and execute processes for disaster recovery and business continuity. The range of recovery services covers the spectrum from partial loss of function or data for a brief amount of time to a "worst-case" scenario in which a man-made, natural disaster, or service failure results in the loss of an entire service. Services may be required during any timeframe from initial declaration of a disaster to final recovery of all business processes. Service availability requirements will be specified by individual Task Orders.

3.12 Training

The Contractor shall develop, implement, and execute processes for initial training for use of all services specified by individual Task Orders. The Contractor shall develop and submit to the Government for review training plans, manuals and other training documentation or training aids. Electronic training tools such as video teleconferencing and computer-based training shall be employed to enhance the effectiveness of training materials and courses. Training delivery may be recorded during live delivery to VA; pre-recorded initial training is not acceptable. The Contractor shall submit a detailed

training plan with timelines and schedules, sufficiently detailed to identify user training plans as specified by individual Task Orders.

The Contractor shall develop accompanying electronic user manuals that VA will subsequently make available to new users. The electronic user manuals shall be delivered along with the training manuals. The Contractor shall revise all user manuals as substantial changes are made to the service.

4.0 Service Areas

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

4.1 Program Management, Strategy, and Planning Support Services

The Contractor shall develop plans for and provide Program and Project Management, monitoring and analysis, strategy, enterprise architecture and planning support on an enterprise or individual project level. Program Management support is critical to the organization achieving strategic goals and fulfilling mission requirements within programmatic constraints. Contractor shall address all program / project management aspects identified at the individual TO level.

4.2 Intake Services

The Contractor shall develop, implement, and execute processes for a series of intake services to support the receipt of physical and digital source materials from a variety of sources and methods, including but not limited to:

- Bulk source materials
- U.S. Mail
- Private carrier delivery (e.g., FedEx, UPS, DHL)
- Facsimiles
- Application Programming Interface (API)
- Self-service submissions

Source materials will be received from VA offices and directly from Veterans and other individuals/locations on behalf of Veterans. The Contractor may also retrieve materials from designated VA and other Government facilities.

The Contractor shall take receipt of all deliveries of physical or electronic source materials on the same day as delivered. This receipt shall constitute the acceptance of the source materials and liability for material management by the Contractor, including complete end-to-end traceability.

Source materials may contain Veterans' claims or other claimants' applications that include VA Sensitive Information. All source materials and VA information received during the performance of this contract, whether in physical or electronic format, shall be treated as sensitive information. While in their custody, the Contractor shall securely handle source materials without loss or damage. The Contractor shall minimize the risk of source material damage while source materials are in the Contractor's custody.

4.3 Source Material Tracking Services

While in their custody, the Contractor shall have documented processes for tracking all physical or digital source materials. The Contractor shall develop, implement, and execute processes for an automated tracking service to be utilized by VA authorized users to facilitate tracking and maintaining a chain of custody for all source materials received by the VICCS Contractors as well as all materials previously received and processed that are now in long term storage awaiting disposition.

4.4 Source Material Management Services

Source material management is the process which integrates the flow of source materials, through and out of an organization to achieve a level of service which ensures that the right materials are available at the right place at the time in the right quantity. The Contractor shall develop, implement, and execute processes for managing all activities associated with the materials in their constructive custody. Such activities include, but are not limited to:

- Loading all necessary information related to the materials into tracking services created for that purpose
- Determining and executing necessary steps for compliance with processing plans and physical security of all materials
- Performing any corrective steps necessary in Contractor and VA provided systems and services to allow continued planned processing activities
- Providing information and feedback to the VA and other Contractors related to completed and planned activities

4.5 Conversion Services

Conversion is defined as the process of changing source materials from one form, state, etc., to another. Conversion includes both the scanning of paper source materials and the conversion of digital/electronic or non-paper source materials into pre-defined images. Materials may be hazardous, delicate, or damaged. The Contractor shall develop, implement, and execute conversion services at a Contractor or Government site as specified in individual Task Orders. While in their custody, the Contractor shall securely handle source materials, manage conversion in accordance with published Document Conversion Rules (DCR) or Business Rules without loss or damage, and work collaboratively with the Government to support efficient processing of variable document conversion production rates. The Contractor shall minimize the risk of source materials damage during conversion. If source material is fragile or likely to be damaged when scanned, the Contractor shall maintain procedures for preventing such damage.

The Contractor shall propose efficient and effective methodologies for protecting source material.

The Contractor shall maintain the physical arrangement of source materials until conversion is complete unless otherwise directed within the Business Rules or Document Conversion Rules. Following conversion, the Contractor shall de-prep source materials in accordance with the Business Rules and Document Conversion Rules.

Specifically, in support of this contract, conversion includes:

- Preparing source materials for conversion
- Converting source materials, sufficient for upload to Government image repositories and/or other Contractor services
- Document indexing
- Data extraction
    - Supporting material tracking
    - Supporting automated business process flows
- De-Preparation of materials for transferring to storage awaiting disposition

4.6 Upload and Routing Services

The Contractor shall develop, implement, and execute processes for uploading and routing images and/or associated metadata to multiple image repositories and services provided by other Contractors as specified by individual Task Orders. Performance of this task may include all or part of the tasks listed below:

- Upload to VA's Veterans Benefits Management System (VBMS) or other non-VBMS repository
- Routing to VICCS inbound mail management support service
- Routing to legacy mail handling service
- Routing to external Private Medical Records (PMR) Contractor
- Routing to other Contractor services
- Routing to VICCS Source Material Tracking Service
- Routing to RMS Contractors

4.7 Inbound Mail Management Support Services

The Contractor shall develop, implement, and execute processes for a single access point inbound mail management support service to remotely display, to VA authorized users, images and associated metadata that were created as a part of the conversion services. This service shall interface with services provided by other Contractors as specified by individual Task Orders.

4.8 Rules-Based Processing Service (RBPS)

The Contractor shall develop, implement, and execute processes for an automated RBPS that supports VA's efforts to modernize claims processing capabilities for VA

authorized users. This service shall interface with existing / future VA and Contractor services specified in individual Task Orders.

4.9 Business Processing Services (BPS)

Business Processing Services consist of a series of service transactions to be completed based upon mail received. VA intends to implement BPS for a series of simplified claims and other business-related services, each with varying levels of complexity. The Contractor shall develop, implement, and execute processes for processing transactions utilizing existing VA and other Contractor-created services. These transactions can be initiated from either manual or automated data entry from a variety of forms, or from pre-populated data sets/service call inputs. Services may include, but are not limited to:

- Mail management services (e.g., mail handling, unidentifiable mail resolution, return mail resolution, etc.)
- Claims services (e.g., claims auto-establishment, manual claims establishment, Burial claims processing, Pension claims processing, Dependency claims processing, etc.)
- Business-related services (e.g., failure to upload resolution, redaction services, image splitting, etc.)

4.10 Centralized Outbound Services

Centralized Outbound Services (COS) is required to centralize the printing, mailing or electronic notification of outbound communications generated by VA staff. The Contractor shall develop, implement, and execute processes for centralized outbound services. These services may include, but are not limited to:

- Downloading specific documents from VA repositories
- Letter generation
- Preparing downloaded documents for delivery
- Outbound delivery
- Notifying and presenting to the recipient an electronic image of the specific documents
- Acknowledging receipt of claims-related materials sent to VA by Veterans / claimants / representatives
- Printing and Mailing Services

4.11 Data Transfer Services

The Contractor shall develop, implement, and execute processes for integrating with various VA systems and other Contractor services to support data transfers as required by individual Task Orders. VA will ensure appropriate interface documentation for all VA systems and other Contractor services is made available with each Task Order.

4.12 Graphical Self-Service Report Generation Capability (VA-Accessible) Services

The Contractor shall develop, implement, and execute processes for a business intelligence engine supporting report generation accessible by VA staff. The Contractor shall expose their raw, real-time data to VA to support the generation of real-time reports as needed. Data access shall be extended to agents of the Government.

4.13 Inbound Call Services

The Contractor shall develop, implement, and execute processes for a call intake capability, providing direct access to VA field users, Veteran Service Organizations (VSOs), and other entities as required by individual Task Orders.

4.14 Outbound Call Services

The Contractor shall develop, implement, and execute processes for an outbound call capability, enough to support a pre-defined period of time/call volume specified by individual Task Orders. VA will deliver the Contractor enough contact information for identified recipients as well as the scripted details of the information VA desires to have communicated.

4.15 Integration, Setup, Test, And Validation Services

The Contractor shall develop, implement, and execute processes for the setup, testing, and validation of all services as required by individual Task Orders. The Contractor shall provide systems integration support to include planning, interoperability specifications and analysis, system interface specifications, and service definitions.

The Contractor shall ensure that any specific setup, testing, and validation procedures are fully documented and complete. The Contractor shall establish a test strategy including end-to-end plans, procedures, and testing scenarios. The Contractor shall establish and test Task Order work flows, business rules, policy definitions, and permissions.

As specified by individual Task Orders, the Contractor shall create and utilize development and test environments that will interconnect appropriately with Government and other Contractor created environments for testing of all services being acquired prior to implementation into the Production environment.

Rollout of all services into the Production environment shall be implemented as a phased approach and shall be detailed in all planning documents including regression testing and service rollback contingency plans. Such phased rollouts shall be implemented for any service updates and not be limited to initial capabilities.

4.16 Service Updates

The Government anticipates updates will be required for any Task Order services provided by the Contractor (routine) and when changes occur to systems / services with which the Contractor will interface (non-routine). The Contractor shall develop,

implement, and execute processes for the performance of routine and non-routine service updates as required by individual Task Orders.

Routine service updates shall be implemented on a bi-monthly basis. Bi-monthly means once every two (2) months. Routine service updates include, but are not limited to, approved changes to:

- Intake Services
- SMTS and User Administration
- VICCS Mail Portal and User Administration
- Rules-Based Processing Service
- Centralized Outbound Services

Non-routine service updates are those updates occurring on either an emergent basis or other than bi-monthly basis. When Government systems, or other VICCS Contractor services are updated, either on a regular interval or on an emergent basis, and where the updates impact the Contractor service, the Contractor shall perform corresponding service updates, including database updates, to ensure ongoing operations. These updates include, but are not limited to, approved changes to:

- Interfaces with VA government system(s)
    - Data access service
    - VBMS
    - VA Application Program Interfaces (API)
- Interfaces with DMHS vendor systems(s)
- Interfaces with PMR vendor system(s)
- Interfaces with RMS vendor system(s)
- NARA Registry Database Update (Quarterly)
- eFax Configuration
- Contractor service User Interface (UI) updates

4.17 Data Transition In / Out Services

The Contractor shall develop, implement, and execute processes for the transition-in of data from existing Government Contractor Systems and other Government databases to ensure data preservation. Specific Contractor Systems and databases will be identified in individual Task Orders. Data transition sources include, but are not limited to:

- ICMHS Contractor systems
- DMHS Contractor systems
- Records Management Center – Extraction and Scanning Services (RMC-ESS) Contractor systems
- Centralized Benefits and Communications Management (CBCM) Contractor
- RMS Contractor systems
- Full Service Shipping Contractor systems data stored in VA database

- NARA Registry Database
- Control of Veterans Records (COVERS) system
- Archives and Records Center Information System (ARCIS)

The Contractor shall develop, implement, and execute processes for transitioning-out of all data and information from its production systems detailing dates, tasks, milestones, dependencies, resources, risks and risk management strategy, tools, and data/data structure to meet requirements defined in each Task Order. At the end of the period of performance, the Contractor shall support the transition of all data and information from its production systems to VA or its designated agent as required by individual Task Orders.

4.18 Professional Services

The Contractor shall develop, implement, and execute processes for evaluating services areas and conducting other analyses as required by individual Task Orders. The Contractor shall provide professional services including, but not limited to:

- Design/redesign of VA forms
- Creation and maintenance of Business Rules
- Maintenance of Document Type Identification and Date of Receipt Guides
- Maintenance of a Document Taxonomy
- Creation and maintenance of inbound and outbound correspondence services
- Data Analysis / Business Intelligence
- VICCS Services evaluation

4.19 Help Desk Services

The Contractor shall develop, implement, and execute processes for delivering a full array of services, staff, and expertise to establish, operate and maintain ticketing and help desk services specified by individual Task Orders, addressing service issues experienced by end users. Issues could include but are not limited to:

- Authentication and Account Management
- Service errors
- General "how to" to assist end user with basic service operation

The Contractor is not expected to provide VA processing guidance, but rather to ensure the user is aware of the proper functionality of the Contractor provided service.

5.0 Deliverables

5.1 Products

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

5.2 Rights in Data

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

VA does not require the rights to Contractor software/services provided, rather explicitly owns the VA data that resides within (e.g., images, metadata, transaction/user audit logs) and will require this data upon request or the expiration of the contract.
The Contractor shall provide transactional data to VA and other approved third parties on a defined (i.e., daily) frequency. Although VA has not specified the actual transfer mechanism, this can be done through Contractor to Contractor/VA system integrations, or via other methods such as direct database sharing or SFTP, or other Contractor specific capabilities if VA has the matching capability.

As VA receives inputs from a variety of sources, transaction acknowledgements and status updates will be a part of the data sharing task to provide material provisioning interfaces with successful transaction acknowledgements, and internal stakeholders with data for reporting purposes.

6.0 Security and Privacy

Contractors (which includes 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. Contractors must follow policies and procedures outlined in VA Directive 6500, Information Security Program which is available at: http://www1.va.gov/vapubs and its handbooks to ensure appropriate security controls are in place.

6.1 Information Security and Privacy Security Requirements

The Contractor shall comply with the VA security requirements IAW VA Handbook 6500.6 “Contract Security” and Addendum A of VA Handbook 6500.6. VA Handbook 6500.6 Appendix C “VA Information Systems Security / Privacy Language for Inclusion into Contracts, as Appropriate” is included in Section B.2. Section B.2 may be tailored at the Task Order level.

6.2 Personnel Security Requirements

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

The position sensitivity risk designation [LOW, MODERATE, and HIGH] and associated level of background investigation [Tier 1, Tier 2, and Tier 4] for each Task Order PWS task shall be designated accordingly, as identified within the TO PWS. The level and process of background security investigations for Contractors must be IAW VA Directive and Handbook 0710, “Personnel Security and Suitability Program.”

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 three (3) calendar days after Task Order award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (Refer to Task Order PWS for investigative requirements by task), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or separately to the COR. The Contractor Staff Roster shall be updated and provided to VA within one (1) calendar 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 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 five (5) calendar days after Task Order award:

    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed Security and Investigations Center (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 SF86) 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 three (3) calendar 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 three (3) calendar days that documents were signed via e-QIP).

g. The Contractor shall be responsible for the actions of all personnel (including Subcontractor personnel) provided to work for VA under this contract. If 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. If the background investigation determination is not completed prior to the start date of work identified in each Task Order, a Contractor may be granted access to VA sensitive information 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 the Office of Personnel Management (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 always, and returning the identity credentials upon termination of their relationship with VA.

6.3 Facility/Resource Access Provisions

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external

equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All 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 is 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 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. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems / LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to Addendum A, Additional VA Requirements, Consolidated and Addendum B - VA Information and Information System Security/Privacy Language.

6.4 Badges

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

6.5 Incident Reporting and Management

The Contractor shall inform the COR, VA Program Manager (PM) and assigned local Information Security Officer (ISO) of any security events and the Privacy Officer (PO) for

any privacy violations within one hour of occurrence. Contractor will provide updates on the reported security / privacy events until closed by the ISO/IPO.

Individuals directly involved with and in the leadership chain who fail to adequately report and or provide status in a timely fashion on incidents affecting the integrity and/or security of VA information will be removed from the contract for violations of the Rules of Behavior.

6.6 Security and Privacy Awareness Training

The Contractor shall complete the initial security and privacy awareness training and accept the VA Contractor Rules of Behavior (ROB) in the VA Talent Management System (TMS) within two (2) calendar days of Task Order award. The Contractor shall complete the annual security and privacy awareness training and accept the VA Contractor ROB prior to expiration in the VA TMS.

6.7 Security Role-Based Training

The Contractor shall complete the assigned security role-based training in TMS, within three (3) calendar days following assignment by the COR, as a prerequisite to receiving elevated privileges.

7.0 Contract Management

7.1 Government Support

7.1.1 IDIQ COR

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

7.1.2 Task Order COR

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

7.1.3 Onsite Government Representative

The Government reserves the right to assign a Government representative to a Contractor facility for the duration of any Task Order. Where a Government representative is assigned onsite, full-time space shall include a computer workstation with both network and phone (with outbound calling capability) access and shall be situated in a manner allowing for uninterrupted teleconferences between the representative and VA Leadership. The Contractor shall provide adequate, secure office

workspace located within a climate-controlled area accessible through similar security measures as the Contractor's employees. The representative shall have physical access to the facility such that reviews of any process may be executed on an at-once basis as may be directed by VA.

7.2 Contractor Program Management

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

7.2.1 Key Personnel

Certain skilled experienced professional and / or technical personnel are essential for accomplishing the work to be performed. These individuals are defined as "Key Personnel" and are those persons whose résumés were submitted and marked by the Contractor as "Key Personnel." Key personnel will be identified for individual TOs, if the Government designates positions as being essential or "key" to the work performed under that TO.

7.2.2 Work Control

All program requirements, contract actions and data interchange shall be conducted in a digital environment using electronic and web-based applications. At minimum, such data shall be compatible with the Microsoft Office 365/ Office 16 family of products, Microsoft Windows 7 and Windows 10 products, Adobe Portable Document Format (PDF) and AutoCAD. In coordination with Contractor Task Order PM a standard naming convention for all electronic submissions shall be determined within 60 calendar days after Task Order award.

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), 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. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

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

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

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

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

Additional requirements may be specified at the Task Order level.

A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall always wear visible identification 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, except for software licenses that need to be procured from a Contractor or Contractor 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 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 shall 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 24 hours of any employee termination.

g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".

h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

A6.0 Information Technology Using Energy-Efficient Products

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

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

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements. The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

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

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

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives

2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)

3. Televisions, Multimedia Projectors

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

Addendum B – Performance Based Service Assessment

PERFORMANCE BASED SERVICE ASSESSMENT template is provided For Reference Only

PERFORMANCE BASED SERVICE ASSESSMENT

CONTRACTOR: _____
GOVERNMENT REQUIRING ACTIVITY: _____
CONTRACT/ORDER NUMBER/ TITLE: _____
PERFORMANCE PERIOD COVERED: _____
NAME AND TITLE OF COR: _____
DATE: _____

EVALUATION RATINGS FOR ASSESSMENT

- EXCEPTIONAL
- VERY GOOD
- SATISFACTORY
- MARGINAL
- UNSATISFACTORY

All value ratings must be supported, objective and explained in the Narrative Section for each Performance Objective.

PERFORMANCE OBECTIVES:

A. TECHNICAL / QUALITY OF PRODUCT OR SERVICE: **Rating:** ***<Value>***

How well does the Contractor meet your Technical Requirement IAW the performance metrics in the PWS?

NARRATIVE: ***(Enter narrative in box)***

B. PROJECT MILESTONES AND SCHEDULE: **Rating: *<Value>***

How well does the Contractor meet the established schedule IAW the performance metrics in the PWS?

NARRATIVE: ***(Enter narrative in box)***

C. COST & STAFFING: **Rating: *<Value>***

Are the staffing levels and expertise appropriate for accomplishing the mission IAW the performance metrics in the PWS?

Were the invoices current, accurate and complete?

NARRATIVE: ***(Enter narrative in box)***

D. MANAGEMENT: **Rating: *<Value>***

How well did the Contractor integrate / coordinate all activities needed to execute the contract IAW the performance metrics in the PWS?

NARRATIVE: ***(Enter narrative in box)***