



PERFORMANCE WORK STATEMENT (PWS) DEPARTMENT OF VETERANS AFFAIRS

Office of Small and Disadvantaged Business Utilization (OSDBU)

VA Business Intelligence Tool (VA-BIT)

Date: 02/13/2018

TAC-18-XXXXX

PWS Version Number: 1.5

VA Business Intelligence (VA-BIT)

TAC Number: TAC-18-XXXX

Contents

1.0	BACKGROUND.....	5
2.0	APPLICABLE DOCUMENTS.....	5
3.0	SCOPE OF WORK.....	10
4.0	PERFORMANCE DETAILS.....	11
4.1	PERFORMANCE PERIOD.....	11
4.2	PLACE OF PERFORMANCE.....	12
4.3	TRAVEL or special requirements	13
5.0	SPECIFIC TASKS AND DELIVERABLES	13
5.1	PROJECT MANAGEMENT.....	14
5.1.1	CONTRACTOR PROJECT MANAGEMENT PLAN.....	15
5.1.2	REPORTING REQUIREMENTS	16
5.1.2.1	EPMO STATUS REPORT.....	16
5.1.3	RATIONAL TOOLS TRAINING.....	17
5.1.4	PRIVACY TRAINING.....	18
5.1.5	TECHNICAL KICKOFF MEETING.....	18
5.1.6	ONBOARDING	19
5.1.7	SCHEDULE MANAGEMENT	19
5.1.8	RISK MANAGEMENT.....	20
5.1.9	CONFIGURATION MANAGEMENT	20
5.1.10	PLANNING	21
5.1.10.1	VA-BIT PHASE-IN TRANSITION SUPPORT	21
5.1.10.2	DEVELOPMENT	21
5.1.11	SOFTWARE DEVELOPMENT LIFECYCLE.....	22
5.1.11.1	AGILE REQUIREMENTS ELABORATION.....	23
5.1.11.2	BUILD AND DEVELOPMENT	24
5.1.11.2.1	SOLUTION ARCHITECTURE PLANNING AND EXECUTION.....	24
5.1.11.2.2	INTEGRATION AND PARTNER MANAGEMENT.....	25
5.1.11.2.3	BUILD PLANNING	26
5.1.11.2.4	SPRINT PLANNING	28
5.1.11.2.5	SPRINT EXECUTION	28
5.1.11.2.6	TESTING.....	30
5.1.11.2.7	ENTERPRISE SECURITY CHANGE CONTROL BOARD (ESCCB) AND NETWORK SECURITY OPERATIONS CENTER (NSOC)	32
5.1.11.2.8	SOLUTION TRAINING	33
5.2.1	VA-BIT Standard Features	35
5.2.2	AUTOMATED BACK-END DATABASE ATTRIBUTES	35
5.2.3	DATA SOURCES	36
5.2.4	FEDERAL BUSINESS OPPORTUNITIES REPOSITORY	37
5.2.5	VA-BIT STANDARD REPORTS	38
5.2.6	VA-BIT SEARCH CAPABILITIES.....	40
5.2.7	VA GOALS MANAGEMENT DASHBOARD.....	42
5.2.8	VA-BIT SIMPLIFIED ACQUISITION THRESHOLD (SAT) MANAGEMENT TOOL	44
5.2.9	MARKET RESEARCH ANALYTICAL TOOL	44

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

5.2.10	FedRAMP-APPROVED CLOUD DEPLOYMENT.....	46
5.2.10.1	PROVIDE HOSTING CLOUD ENVIRONMENTS.....	47
5.2.10.2	PROVIDE NETWORK CONNECTIVITY	49
5.2.10.3	DATA MIGRATION SOFTWARE AND SUPPORT.....	51
5.2.10.4	HOSTED GFE (HGFE) SERVICES.....	51
5.2.10.5	OBTAIN AND MAINTAIN AUTHORITY TO OPERATE (ATO)	52
5.3	Integration into a Third-Party Applications/Web Services/Application Programming Interfaces (APIs) (PHASE II)	54
5.3.1	VA-BIT INTEGRATION TEAM.....	55
5.4	Development of Vendor Capabilities (Optional Task) – (PHASE III)	56
5.4.1	VA-BIT VENDOR DASHBOARD FEATURES	56
5.4.2	RELEASE AND DEPLOYMENT	62
5.4.2.1	PRE-RELEASE SUPPORT.....	62
5.4.2.2	INITIAL OPERATING CAPABILITY (IOC) SUPPORT	63
5.4.2.3	RELEASE AND DEPLOYMENT SUPPORT	64
5.5	ADDITIONAL VA-BIT DEVELOPMENT (OPTIONAL TASK 2)	65
5.5.1.1	WARRANTY SUPPORT	66
5.5.2	OPERATIONS AND MAINTENANCE SUPPORT	66
5.5.3	OPERATIONS AND MAINTENANCE SUPPORT (OPTION PERIODS ONLY)	67
5.5.4	CHANGE AND CONFIGURATION MANAGEMENT SUPPORT	68
5.5.5	APPLICATION SUPPORT/END USER MANAGEMENT.....	69
5.5.6	MAINTENANCE RELEASE DEPLOYMENT MANAGEMENT	69
5.5.7	DATABASE ADMINISTRATION SUPPORT.....	70
5.5.8	DATABASE MIGRATION SUPPORT	70
5.5.9	OPERATIONAL SUPPORT	71
5.5.10	TESTING SUPPORT	77
5.5.11	TECHNICAL SUPPORT.....	77
5.5.12	TECH REFRESH	78
5.5.13	COTS SOFTWARE PATCHES	78
5.5.14	SERVICE DESK SUPPORT.....	78
5.5.14.1	TIER 2 SUPPORT	79
5.5.14.2	TIER 3 AND 4 SUPPORT	80
5.5.14.3	SERVICE DESK DOCUMENTATION AND REPORTING.....	81
5.6	PHASE-OUT TRANSITION SUPPORT	82
6.0	GENERAL REQUIREMENTS.....	83
6.1	ENTERPRISE AND IT FRAMEWORK.....	83
6.2	SECURITY AND PRIVACY REQUIREMENTS	85
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S)	87
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS.....	88
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES	89
6.4	PERFORMANCE METRICS	90
6.5	FACILITY/RESOURCE PROVISIONS.....	91
6.6	GOVERNMENT FURNISHED PROPERTY	92
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED	93

DRAFT

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Small and Disadvantaged Business Utilization (OSDBU) provides services to Veteran Owned Small Businesses (VOSB) and Service-Disabled Veteran Owned Small Businesses (SDVOSB) who seek to gain access to economic opportunity by leveraging the Federal procurement system.

To meet the requirements of Public Law 109-461, VA verifies the eligibility of firms registered in the Vendor Information Pages (VIP) database to ensure they are owned and controlled by Veterans or Service-Disabled Veterans. The VIP database was established to assist VA acquisition personnel verify the eligibility of firms seeking to participate in the VA procurement process. OSDBU also provides outreach and liaison support to businesses (small and large) and other members of the public and private sectors concerning Small Business Acquisition issues. OSDBU is responsible for monitoring the Department of Veterans Affairs (VA) implementation and execution of the socioeconomic programs.

OSDBU intends to procure a customizable cloud-based Software as a Service (SaaS) solution to address market research, market intelligence, analytics, and reporting services to aid Procurement Decision Makers (PDM's), Program Offices, Contracting Officers, Vendors, and other VA officials in conducting detailed, compelling, and defensible market research. The solution to be called the VA – Business Intelligence Tool (VA-BIT) will support hundreds of concurrent users creating, accessing and reporting thousands of requirement and procurement records. VA-BIT shall support the market intelligence and information needs of stakeholders at all levels who access data from both VA and external systems. VA-BIT shall utilize a variety of business intelligence techniques to present data for decision making including: metrics and key performance indicators, dashboards with graphical displays, interactive reports and self-service ad-hoc reporting. VA-BIT addresses the VA's need to build a collaborative market intelligence platform where stakeholders at all levels across the organization have access to timely and accurate information required for market research, performance measurement, and enhanced decision-making. With VA-BIT, VA-BIT will be able to integrate core market research and intelligence data with a wide variety of internal and external data sources to support the VA

OSDBU plans to continue executing VA-BIT enhancements in phases to expand the use of business intelligence, with the goals of further enhancing market research, market intelligence, information sharing, reporting, as well as facilitating effective decision making.

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"

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

2. Office of Management & Budget (OMB) Memorandum M-14-04, "FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," November 18, 2013 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 Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
9. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
10. VA Directive and Handbook 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, "Managing Federal Information as a Strategic Resource," July 28, 2016
13. Office of Management & Budget (OMB) Circular A-130 Appendix III, "Transmittal Memorandum #4, Management of Federal Information Resources"
14. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
15. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
16. 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
17. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
18. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
19. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
20. Department of Veterans Affairs (VA) Handbook 6500.1, "Electronic Media Sanitization", 2012
21. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
22. Department of Veterans Affairs (VA), Office of Information and Technology (OIT), Corporate Data Center Operations (CDCO), Austin Information Technology Center (AITC), Handbook 6500.02, "Computer and Network Security Incident Response", January 6, 2012

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

23. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
24. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
25. VA Handbook 6500.6, "To Security," March 12, 2010
26. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
27. OI&T ProPath Process Methodology (Transitioning to Process Asset Library (PAL) (reference process maps at <http://www.va.gov/PROPATH/Maps.asp> and templates at <http://www.va.gov/PROPATH/Templates.asp>
28. One-VA Technical Reference Model (TRM) (reference at <http://www.va.gov/trm/TRMHomePage.aspx>)
29. National Institute Standards and Technology (NIST) Special Publications (SP)
30. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
31. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
32. Department of Veterans Affairs (VA) Directive 6300, "Records and Information Management", 2012
33. Department of Veterans Affairs (VA) Handbook 6300.1, "Records Management Procedures", 2012
34. OMB Memorandum, "Transition to IPv6", September 28, 2010
35. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
36. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
37. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
38. 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
39. 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
40. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
41. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
42. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
43. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
44. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXX**

45. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
46. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
47. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
48. 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>)
49. 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>)
50. 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>)
51. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
52. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
53. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
54. 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>)
55. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
56. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
57. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
58. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
59. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
60. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
61. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
62. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
63. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

64. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
65. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
66. "Veteran Focused Integration Process (VIP) Guide 1.0", December, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
67. "VIP Release Process Guide", Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
68. "POLARIS User Guide", Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
69. Department of Veterans Affairs (VA), Office of Information and Technology (OIT), "Process Management Change Control Process Guide", V1.1, December 2010
70. Department of Veterans Affairs (VA), Office of Information and Technology (OIT), Service Delivery and Engineering (SDE), "VA Enterprise Disaster Recovery Service Tiers and Technology Solutions Standards", Version 1.0, September 2012.
71. Department of Veterans Affairs (VA), Office of Information and Technology (OIT), Office of Cyber Security (OCS), "VA Authority to Operate Requirements", April 2013
72. Distributed Management Task Force (DMTF), "Open Virtualization Format Specification", Version 1.0, 2009
73. Electronic Industries Alliance (EIA) Standard EIA-310-D (rev. E), Cabinets, Racks, Panels, and Associated Equipment, 1996
74. Federal Information Process Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
75. National Archives and Records Administration (NARA), "Basic Laws and Authorities", February, 2008 Revision, "Basic Laws and Authorities of the National Archives and Records Administration", 2006 Edition
76. Office of Management & Budget (OMB) Memorandum M-14-30, "Security Authorization of information Systems in Cloud Computing Environments," December 8, 2011
77. National Institute Standards and Technology (NIST) 800-53 MP-1 (Rev. 4), "Media Protection Policy and Procedure," April 28, 2013
78. Federal Risk and Authorization Management Program (FedRAMP), "FedRAMP Standard Tonal Clauses", June 1012
79. NIST Special Publication 500-291, "NIST Cloud Computing Standards," Version 2, July 2013
80. NIST SP 800 146, "The NIST Definition of Cloud Computing"

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

3.0 SCOPE OF WORK

The Contractor shall provide all resources necessary to accomplish the deliverables as described in this Performance Work Statement (PWS). The proposed effort is to offer a customizable SaaS solution to aid Procurement Decision Makers (PDM's) and other VA stakeholders in conducting detailed, compelling, and defensible market research to identify potential Service-disabled Veteran Owned Small Business (SDVOSB's) and/or Veteran-owned Small Business (VOSB) concerns in order to meet the agency's small business goals. In addition to managing the small business goals, the SaaS solution will help PDM's in identifying strategic sourcing vehicles, as well as helping VA OSDBU in monitoring all contracting activity for the purposes of gaining analytical perspectives for better decision-making towards achieving its goals. This acquisition will overcome the challenges of collecting timely information to perform adequate market research in order to maximize competition among capable Contractors. The proposed solution shall also address the agency ability to perform market research, market intelligence, analytics and reporting needs. The solution to be called the VA-Business Intelligence Tool (VA-BIT) will support hundreds of concurrent users creating, accessing and reporting thousands of requirement and procurement records.

VA-BIT shall provide turnkey cloud-based, web-based Software-as-a-Service (SaaS). The SaaS solution shall include configuration, upgrades, software patches, updates, helpdesk support and architectural support to sustain and expand VA-BIT suite. VA-BIT shall deliver business functionality through a number of configured applications to key stakeholders. VA-BIT shall meet the rigorous security standards of VA including Federal Risk and Authorization Management Program (FedRAMP), Trusted Internet Connection (TIC) compliant, Identity and Access Management services for single sign-on internal and external, as well as enable the integration of external data sources, web services, and/or Application Programming Interfaces.

End Users of VA-BIT will include the following:

- Acquisition Professionals (AQP)
- Small Business Professionals (SBP)
- Program Office Professionals (POP)
- Contracting Office Professionals (COP)
- General Staff Users (GSU)
- External Data Users (DUR)
- Procurement Decision Makers (PDM)
- Agency Administrators (AA)
- Industry Engagement Professionals (IEP)
- Senior Procurement Council Members (SPC)
- Acquisitions and To Administrators (ACA)
- Office of Small Disadvantaged Business Utilization (OSDBU)
- Small Business Liaison Professionals (SBL)
- Potential Contractors: Small (SB) and Other-than-Small Businesses (OTSB)

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The base Period of Performance (PoP) is 06/27/2018 – 06/26/2019 with four (1) one-year option periods. Work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO).

OSDBU anticipates work will be completed in the following phases. OSDBU reserves the right to modify the number of phases.

Phase I (03/01/2018 – 06/30/2018): Task 5.2, VA-BIT Procurement Decision Maker (PDM) Capabilities on On-Premise or FedRAMP-Approved Cloud Deployment

The Government expects full operational capability of all requirements outlined in Task 5.1 to be completed within 4 months of contract award. At the close of Phase 1, the Contractor will deliver to the government for review and acceptance of the User Acceptance Test (UAT) results necessary to demonstrate a high likelihood of success for delivery of the services identifying any deficiencies evidenced in documentation and as a result of service and user acceptance testing.

Phase II (07/01/2018 – 09/30/2018) Task 5.3, Integration into a Third-Party Applications/Web Services/Application Programming Interfaces (APIs)

Within 15 days of notification by the government of Phase II acceptance, the Contractor shall begin configuration and implementation of Task 5.3 to ensure a full implementation no later than 2 months after Phase II completion.

Phase III (10/01/2018 – 02/28/2019) Task 5.4, Development of Vendor Capabilities (Optional Task 1). This task allows for the development of vendor-facing capabilities of the VA-BIT application. If exercised, work on this optional task will commence during the base period on 10/01/2018. Work on this optional task may continue throughout the remaining option periods.

Task 5.5, Optional Task 2, Additional VA-BIT Development. This task allows for further development of the VA-BIT application. If exercised, the period of performance for this optional task will commence any time during the option period.

Task 5.6, Operations and Maintenance. This task provides for operations and maintenance of the VA-BIT application throughout the entire life of the contract. This task shall commence in the base period with the production deployment of Phase I.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

4.1.1 PLACE OF PERFORMANCE

4.1.2 EFFORTS UNDER THIS PWS SHALL BE PERFORMED IN VA FACILITIES LOCATED IN WASHINGTON, DC AND AT THE CONTRACTOR'S FACILITY. THE MAJORITY OF THE EFFORT SHALL TAKE PLACE AT THE CONTRACTOR'S FACILITY. IT IS ANTICIPATED THAT SOME KEY CONTRACTOR SUPPORT PERSONNEL (SUPPORTING PROJECT MANAGEMENT, STRATEGIC DESIGN DISCUSSIONS/WHITEBOARDING EXERCISES, SENIOR LEADERSHIP MEETINGS, AND COLLABORATION DISCUSSIONS WITH TECHNICAL TEAMS) WILL BE LOCATED IN WASHINGTON, DC. CONTRACTORS SHALL BE REQUIRED TO TRAVEL TO OTHER LOCATIONS AS SPECIFIED IN SECTION 4.3.

4.1.3 WORK BY KEY CONTRACTOR PERSONNEL LOCATED IN WASHINGTON, DC MAY BE PERFORMED AT REMOTE LOCATIONS WITH PRIOR CONCURRENCE FROM THE CONTRACTING OFFICER'S REPRESENTATIVE (COR).

4.1.4 THE CONTRACTOR SHALL OPERATE WITHIN NORMAL BUSINESS HOURS ON EASTERN STANDARD TIME (6:00 A.M. TO 10:00 P.M. EST). THE CONTRACTOR SHALL PROVIDE 24/7 OPERATIONS 365 DAYS PER YEAR AS IDENTIFIED IN SECTION 5.5.9.

Work at a Government site shall not take place on Federal holidays or weekends (but may require off-hour work due to network loading or other disruptions that could occur) unless specifically approved in advance by the COR. There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

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

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

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

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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

4.1.5 TRAVEL OR SPECIAL REQUIREMENTS

The Government anticipates travel to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Travel and per diem shall be in accordance with the Federal Travel Regulations (FTR) and requires advanced concurrence by the COR with VA Program / Project Manager's concurrence. The Contractor shall provide cost estimates with each travel request. Each Contractor invoice must include copies of all receipts that support the travel costs claimed in the invoice. Local travel within a 50-mile radius from the Contractor's normal duty location is considered the cost of doing business and will not be reimbursed. This includes travel, subsistence, and associated labor charges for travel time. Travel performed for personal convenience and daily travel to and from work at the Contractor's facility will not be reimbursed. Travel, subsistence, and associated labor charges for travel time for travel beyond a 50-mile radius of the Contractor's facility are authorized on a case-by-case basis and must be pre-approved by the COR.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following tasks and provide the specific deliverables described below within the performance period stated in Section 4.1 of this PWS.

Each integration and development activity shall be performed via a common SDLC process and contribute to the analysis, design, construction, testing, and deployment efforts using VA release management processes and artifacts.

The scope of this order shall include the following Work Breakdown Structure activities:

- a. Project Management
- b. Software Development for projects using Agile SDLC processes
- c. Testing and release
- d. Operations and Maintenance (O&M) Support
- e. Transition Support

The Contractor shall provide development and also perform operations and maintenance support services using existing code, for code developed under this PWS and potentially code developed outside of this PWS.

All tools used in the maintenance of the VA-BIT application and related applications must be approved in the Technical Reference Manual (TRM). Deviations from this will require a waiver through the Strategic Technology Alignment Team (STAT), formerly known as the Architecture and Engineering Review Board (AERB). Request for exceptions or deviations cannot impact delivery. All tools used in the environments of VA-BIT and related Programs and all applications produced by VA-BIT and related program projects shall be VA Section 508 compliant as determined by tests performed by the VA Section 508 Office.

Agile project management is evolutionary (iterative & incremental) which regularly produces high quality results in a cost effective, timely, and highly collaborative manner

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

via VIP's value driven lifecycle. This requires open lines of communication among all participants contributing to a project/program/portfolio that include multiple consumers within the contracts and with other VA offices/activities.

VIP describes a schedule of incremental deliveries of useable functionality every three (3) months or less.

All releases into the production environment shall come through the VIP Release Process. It is critical to work with the VA Release Agent on a regular basis in order to understand the required components of the Release Readiness Review (RRR) Process.

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance.

The foundational structure for VA Agile development and project management can be found in the VIP Guide. For delivery of all project artifacts, the Contractor shall utilize Rational for managing project execution details and for the management and storage of artifacts using approved VIP and/or EPMO website templates.

The Contractor shall utilize approved VIP and/or Process Asset Library (PAL) (formerly ProPath templates). When no VIP or ProPath template exists, the Contractor shall design and develop a template to be utilized for all tasks being developed under this PWS that must be reviewed and approved by the VA COR prior for delivery of the associated artifact. The Contractor shall include only the content and artifacts that have been updated or developed in the target increment/build in deliverable packages. When no change to a package component has occurred during an increment/build, unrelated or unchanged artifacts will not be included in the associated delivery packages. The Contractor shall provide a revision history with track changes on to allow for easy visibility of changes between package deliverables. Although not all project artifacts will require an update for each release, the Contractor shall ensure that all necessary artifacts are delivered to the appropriate VA governance committees as mandated by VA-established release processes. If a project artifact doesn't require an update, the Contractor shall provide justification to the VA Project Manager and / or COR for approval.

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

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

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

The CPMP shall describe the technical approach, timelines, organizational resources, and management controls being employed to meet the cost, schedule, and performance requirements as defined in this PWS. The CPMP shall describe the resource organization structure as well as the processes to establish, organize, and maintain effective resources to support project activities. The CPMP shall include the following:

- A Quality Assurance (QA) plan shall serve as the foundation upon which the Build Test Plan (See Section 5.2.2.3) will be based. The Contractor shall describe the overall approach to QA activities for the project, but shall not include specific testing. This QA Plan shall document how testing will occur, not what will be tested. This plan shall document how the Contractor defines, implements, and assures quality for all project deliverables. System Assurance, including testing of software code, shall be documented in the Build Test Plan.
- A System Communication Management Plan which shall describe the processes that will be used to ensure timely and appropriate generation, collection, dissemination, storage, and ultimate disposition of project information (to include processes for the dissemination of information regarding system outages and updates and/or fixes). The processes should provide the links between stakeholders, ideas, and information that will be necessary for project success. The System Communication Management Plan component of the CPMP shall identify processes for ensuring succinct, responsive, and timely messaging during critical events or issues that may be encountered by the project.
- The Contractor shall deliver a Hosting Solution Plan that details the contractor approach to providing a flexible, scalable processing, memory and storage capacity. The plan shall provide both data for Standard and Premium performance storage to the capacities, and hypervisor functionality requirements and Service Level Agreement (SLA) for expected performance of virtualization (see additional information in sections 5.3 and Appendix B). The Contractor shall provide updates to the Hosting Solution Plan that encompasses their approach to successfully deliver all functionality for items a though o outlined in section 5.2.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- The Contractor shall deliver a Transition Management Plan (TMP) that lays out the Contractor's approach, timeline and tools to be used in the transition of the subject project. The TMP sub-section shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The initial TMP sub-section shall be concurred upon and updated weekly throughout the transition and the initial certification process.

Deliverables:

- A. Contractor Project Management Plan

5.1.2 REPORTING REQUIREMENTS

5.1.2.1 EPMO MANAGEMENT

The Contractor shall use the VA's Rational Toolset to provide a single Agile product lifecycle management tool to track execution details. The Rational product Data and Artifact Repository will be used to provide a single authoritative product data source and artifact repository. All OI&T project data and artifacts will be required to be managed in Rational on a daily basis. All checked out artifacts shall be checked back in before the end of each business day. Rational synchronizes all changed information immediately for all team members in support of configuration management and to ensure work is being done on the most updated information.

The Contractor shall use VA Rational tools in accordance with the VA Rational Tools Guide to:

- Input and manage scheduled product sprints and backlog;
- Input and manage epics, user stories, and requirements;
- Input and manage product risks and issues;
- Input and manage product configurations and changes;
- Input and manage product test plans and execution;
- Input and manage product planning and engineering documentation;
- Input and manage linkages between requirements, code, tests and defects to correlate requirements to change orders to configurable items to risks, impediments, and issues to test cases and test results to show full traceability.

The Contractor shall enter all Agile requirements, changes, tests performed and test results in Rational to show evidence of code coverage and test coverage of all the requirements specified. This will allow VA to have high confidence in a fully documented requirement, as evidenced by data in the Rational Team Concert (RTC) tool and/or the Requirements Traceability Matrix (RTM).

5.1.2.1 EPMO STATUS REPORT

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

The Contractor shall deliver Bi-Weekly (every two weeks) EPMO Status Reports detailing the status of all work efforts. These reports shall provide accurate, timely, and complete project information supporting EPMO reporting Requirements. The Bi-Weekly Status Report shall include the following data elements:

- Project Name and TO
- Overview and description of the TO
- Overall high level assessment of TO progress
- All work in-progress and completed during the reporting period
- Identification of any TO related issues uncovered during the reporting period and especially highlight those areas with a high probability of impacting schedule, cost or performance goals and their likely impact on schedule, cost, or performance goals
- Explanations for any unresolved issues, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution
- Status on previously identified issues, actions taken to mitigate the situation and/or progress made in rectifying the situation
- Work planned for the subsequent four reporting periods, when applicable
- Current TO schedule overlaid on original TO schedule showing any delays or advancement in schedule
- Current definition of user requirements / function points overlaid over the original function points and the last reported function points to specifically identify changes in the function points to be delivered since the previous report
- Workforce staffing data showing all Contractor personnel performing on the effort during the current reporting period. After the initial labor baseline is provided, each Bi-Weekly Status Report shall identify any changes in staffing identifying each person who was added to the contract or removed from the contract
- Original schedule of deliverables and the corresponding deliverables made during the current reporting period

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

Deliverables:

- B. Bi-Weekly EPMO Status Report

5.1.3 RATIONAL TOOLS TRAINING

The Contractor and Government Project Manager shall determine which team members require access to the Rational Tool Suite. All Contractors that require access shall complete all of the following VA Talent Management System (TMS) training courses

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

within 14 days of the identification of the access need. The Contractor shall work with their respective point of contact, to obtain access of the TMS to take the mandatory training courses listed below:

- TMS ID 3878248 - IBM Rational Team Concert - Agile Sprint, Configuration/Change Management Level 1
- TMS ID 3878249 - IBM Rational Team Concert - Agile Sprint, Configuration /Change Management Level 2
- TMS ID 3878250 - IBM Rational DOORS Next Generation - Requirements Management Level 1
- TMS ID 3897036 - IBM Rational DOORS Next Generation - Requirements Management Level 2
- TMS ID 3897034 - IBM Rational Quality Manager - Quality Management Level 1
- TMS ID 3897035 - IBM Rational Quality Manager - Quality Management Level 2

Contractors who have completed these VA training courses within the past 24 months, and have furnished training certificates to VA, will not be required to re-take the training courses.

Deliverables:

C. Rational Training Certificates

5.1.4 PRIVACY TRAINING

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

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

Deliverable:

- D. TMS Training Certificates
- E. Signed Contractor Rules of Behavior

5.1.5 TECHNICAL KICKOFF MEETING

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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

meeting minutes (shall be provided to all attendees within three calendar days after the meeting). The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PMs.

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

Deliverable:

F. Technical Kickoff Meeting

5.1.6 ONBOARDING

The Contractor shall manage the onboarding of its staff. Onboarding includes steps to obtain a VA PIV card, network and email account, complete training, initiate background investigations, and gain physical and logical access. In addition, the Contractor shall identify individuals which may require elevated privileges to the necessary development and test environments for the various systems to be enhanced. After review between the Contractor and VA COR, a decision will be made as to the necessity of obtaining GFE for the onboarding staff. If approved, Contractor shall follow the appropriate steps to obtain the equipment.

A single Contractor Onboarding POC shall be designated by the Contractor that tracks the onboarding status of all Contractor personnel. The Contractor Onboarding POC shall be responsible for accurate and timely submission of all required VA onboarding paperwork to the VA COR. The Contractor shall be responsible for tracking the status of all their staff's onboarding activities to include the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, and their next required training date. The Contractor Onboarding POC shall also report the status at the staff level during onboarding status meetings. The Contractor shall provide an Onboarding Status Report weekly for any staff with outstanding onboarding requests for review by the COR, VA PM and Project Manager.

Deliverable:

G. Weekly Onboarding Status Report

5.1.7 SCHEDULE MANAGEMENT

The Contractor shall create, maintain, analyze, and report integrated schedules. The schedules shall have a minimum of five Work Breakdown Structure levels for their activities. A schedule shall be developed / reviewed / revised for each build and sprint. The Contractor shall provide schedule updates in Rational on a weekly basis. The Contractor shall also provide an updated Project Schedule (in PDF and MS Project

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

format) as input to the VA- maintained Program Integrated Master Schedule (IMS), at a minimum once a week.

Deliverable:

H. Updated Project Schedule

5.1.8 RISK MANAGEMENT

The Contractor shall conduct risk management of all work performed under this TO and provide input to the product Risk Management registry within Rational maintained by VA.

The Contractor shall:

- Report, monitor, manage and mitigate risks for each respective product
- Enter and update risks in the VA approved Risk Repository.
- Assess the status of its risks on a weekly basis and provide them to VA for inclusion in the larger Risk Management Registry. When new risks occur which could impact development, testing and deployment schedule, the Contractor shall notify the COR and VA PM via email within 24 hours. Email subject line shall read "{Project Name} Risk Alert Notification"
- Provide the COR and VA PM / PMs a weekly risk report

Deliverable:

I. Weekly Risk Management Status Report

5.1.9 CONFIGURATION MANAGEMENT

The Contractor shall:

- Identify the standard and unique aspects of configuration management to be performed for each project by establishing a Configuration Management (CM) Plan which meets EPMO CM plan requirements. The Contractor shall reflect all CM required activities and standards in each project-level CM plan while determining the unique aspects of the project which require individualized procedures;
- Deliver a list of configuration items to be placed under configuration and change control, which shall be documented in the Configuration Management Plan. The Contractor shall identify types of configuration items pertaining to each product to be placed under configuration management. Based on EPMO requirements, and the unique needs or nature of each project, the Contractor shall determine the components within each project that must be under configuration control;
- Use Rational Team Concert as the VA approved tool and repository for all software source code and electronic artifact configuration and version

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

management. The Contractor shall use the IBM Rational Team Concert tool to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes;

- Ensure all project software and non-software artifacts are versioned correctly and follow a build/release promotion versioning approach which identifies all major, minor, and updated changes to the components;
- Project and Product Artifacts must be baselined and versioned in the Rational CM repository in order to allow the tool to show active and past histories of the check-ins and check-outs of all software components, data, and software product engineering documents. Maintain all baselines of software, software builds, and electronic artifacts in the repository, labeling updates and versions according to published CM procedures;
- Develop, verify and submit with all project build deliveries, a Version Description Document that conforms to EPMO Website standard templates and addresses the manifest of the contents of all software builds created for project releases outside the development environment;
- Establish and maintain status reporting on change and configuration management activity, and ensure Rational Team Concert data records and artifacts are filed and updated daily.

Deliverables:

- J. Configuration Management Plan
- K. Version Description Document

5.1.10 PLANNING

5.1.10.1 VA-BIT PHASE-IN TRANSITION SUPPORT

The Contractor shall execute planning activities including Contractor onboarding activities, required training, project planning activities, documentation review and architectural analysis. In addition, the Contractor shall conduct the Agile requirements elaboration activities.

5.1.10.2 DEVELOPMENT

The Contractor shall provide a scrum team to support all the services and deliverables identified including all subparagraphs, for delivery of system enhancements during the base period. For planning purposes, The specific scope of functionality to be delivered for each release in the base period may include these or other backlog items and will be determined with VA Product/Project business owners prior to the start of each release cycle based on current business priorities. It is anticipated that the level of effort and mix of resources (i.e., scrum teams) necessary to complete each release will remain consistent through the base period releases. The Contractor shall provide at least 1 scrum team). An individual Scrum team shall be comprised of the appropriate

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

distribution of cross functional roles that include (at a minimum) a Scrum Master, developers, quality assurance and tester(s). A Scrum Team may have one (1) or two (2) Technical Leads as part of the team that provide technical guidance, resolve technical impediments and develop source code. Each Scrum Team shall include at least one resource with expertise and experience with implementing the SaaS solution. Each Scrum Team shall also include a dedicated resource that is capable of elaborating complex requirements. A Certified Scrum Master is recommended per team; however, Certified Scrum Masters may be shared across two when appropriate size and technical leadership is available. The Contractor shall provide development management resources to support each release cycle, to include defect management following the release of all software into production.

The Contractor shall establish a VA-BIT Integration Team that shall be responsible for planning and overseeing integrations across each task as well as developing reusable code components/web parts to be consumed by other OSDBU platform applications.

There are various integrations and interfaces across the OSDBU Platform applications; many of which are currently in place or in progress and others that will be required in the future. As there are dependencies on web service providers and other groups within VA that are external to the VA-BIT Program, it has historically been a challenge to provide sufficient planning and lead time in terms of identifying future integration requirements, submitting web service/interface requests to external groups, developing reusable code components/web parts to consume web services, receiving web services from external groups, and implementing integrations in Production within the planned Build timeframes; hence, the need for a dedicated VA-BIT Integration Team to oversee and plan for integrations across each task. The Integration Team shall be capable of developing both web and non-web based interfaces with various VA and external systems and must be staffed sufficiently enough to accept work from multiple projects simultaneously without schedule blocking. At a minimum, the Integration Team shall consist of at least five (5) dedicated members: a Project Manager or Technical Lead to run/oversee the Integration Team, at least one (1) VA-BIT Architect possessing expertise with implementing the web-based version of the SaaS solution at least one (1) Technical Analyst that can elaborate interface requirements as needed, and at least one (1) dedicated Developer. It is expected that Developers assigned to the individual development tasks will be required to provide input to the Integration Team on a regular basis.

Deliverable:

- L. Reusable code components/web parts

5.1.11 SOFTWARE DEVELOPMENT LIFECYCLE

The Contractor shall provide scrum teams to follow the Agile methodology as described below and in the VA VIP guidelines. Scrum teams for this effort shall be composed of an evolving mix of technical skill sets as required to meet the necessary stage of the software development lifecycle and technical nature of the project. The Contractor shall

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

adjust deliverables and Rational updates to match the nature of the software product under development.

5.1.11.1 AGILE REQUIREMENTS ELABORATION

The Contractor shall complete an initial backlog grooming session with the VA team to properly understand and elaborate business Agile requirements. These sessions shall include participants from the business customer, OI&T and system Subject Matter Experts (SMEs). The Contractor shall provide an agenda and minutes for each requirements gathering session to the VA project manager as well as the participants. The outcome of this session shall be a complete review of, and agreement to, the initial user stories, including user stories added as a result of backlog grooming by decomposing epics into stakeholder needs, business requirements, business rules, requirements visualizations and user story elaborations. Product backlog grooming and prioritization are continued throughout the product life cycle and shall be facilitated by the Contractor.

The Contractor shall:

- Ensure all products in the development pipeline are included and executed as appropriate within the overall Agile backlog grooming effort.
- Populate the backlog during an initial planning session identifying all features the team considers relevant to building the product. The backlog serves as the primary source for all program requirements and user stories, and the team shall prioritize the contents.
- Identify and document possible pain points, functionality/platform gaps and opportunities for system enhancements for inclusion in the backlog.
- Facilitate any stakeholder briefings, meetings and/or elicitation sessions.
- Execute requirements reviews with stakeholders and record results of reviews using Rational, updating requirements data as a result of the reviews.
- Complete a Requirements Package that includes all Epics, stakeholder needs, visualizations, stories, and other sources of requirements information for functional and non-functional requirements. The Requirements Package shall also include mock-ups, visual aids, and dynamic wireframes as required to demonstrate the navigation, taxonomy, menus and dependencies between features in the user interface (UI) and all aspects of the presentation layer that interact with the user.
- Input and maintain all requirements data in Rational. Ensure all requirements data is under change control and is fully linked to work items that show traceability to design changes, configurable items, test cases and test results.

Deliverable:

- A. Requirements Package

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

5.1.11.2 BUILD AND DEVELOPMENT

Based on the scope of work established in the Backlog, development builds shall be three (3) months or less. The Contractor shall develop and deliver a Build Plan in collaboration with the project team prior to beginning the build. The Build Plan is the scope of work which will be completed in the agreed upon build timeframe. Each build ends with a new release or push to production. The Contractor shall follow the standard development cycle as outlined below in Section 5.2 and all subparagraphs – Plan, Develop, Test, Release, Performance Monitoring and Warranty for all builds.

A build will consist of a series of sprints (typically 1-4 weeks duration). The Contractor shall provide a Sprint Plan prior to the beginning each Sprint which defines the work to be completed during the Sprint. Once the Sprint Plan is approved by the Government, the Government will establish when the sprint is complete.

The Contractor shall continuously support the iterative build and development methodology in order to complete all epics and user stories identified in the backlog.

5.1.11.2.1 SOLUTION ARCHITECTURE PLANNING AND EXECUTION

The Contractor shall create a Solution Architecture Package that includes the initial business, systems, application, and data architectures for the new features and capabilities using an architecture framework, to be approved by the VA PM/COR. These documents shall be updated utilizing VIP or PAL (formerly ProPath) templates, and Rational when appropriate, and approved by the VA COR/VA PM for each subsequent Sprint. Each subsequent update shall include a Change Page, which specifies the updates made to the document for review and approval by the VA COR/VA PM. The Contractor shall also outline any initial gaps, questions or challenges that may hinder progress in future Builds or Sprints.

The Contractor shall:

- Support the setup of all needed development and test environments to complete required build development and testing. Coordinate with VA to ensure alignment with all development and test environments. The Contractor shall work with VA to ensure required specifications are provided no later than 30 days prior to environment need date;
- Support the VA Authority to Operate (ATO) to obtain/maintain approval, as required. Required ATOs must be obtained prior to build release and ATO approval timelines, including time to complete all necessary security scanning and remediation. The project ATO process must be considered in build planning activities and included in the project schedule.
- Develop and deliver automated build and automated publishing capabilities to schedule jobs and support continuous integration for every sprint. Automated build tools shall be in compliance with the approved list from the One-VA TRM. Code shall be demonstrable and stable enough to be promoted to another

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

environment without issue by evidence of the status of tests and results found in the Rational Tools.

Deliverable:

B. Solution Architecture Package

5.1.11.2.2 INTEGRATION AND PARTNER MANAGEMENT

VA-BIT shall collaborate and integrates with a variety of systems and stakeholders and requires coordination and management of these partner engagements. The Contractor shall support partner management, coordination and integration efforts.

The Contractor shall:

- Develop a Partner Integration Strategy Plan on how VA-BIT applications can integrate with and consume services provided by partners, as well as share data with other VA applications per backlog requirements as part of the Partner Integration Plan. The Partner Integration Plan shall include an overview of the systems, a description of the major tasks involved in the integration of system components, the roles and responsibilities of integrating teams and organization, integration resources and the integration strategy that is to be supported;
- Coordinate integration and releasing activities to include dependencies with partner services, scheduling, and trigger dates;
- Collaborate with project partners, which may include other vendors, to establish the priority, scope, bounds, and resources and manage and mitigate project risks and issues regarding trigger dates and dependencies, blockers and proper escalation mechanisms;
- Manage and coordinate touch points with critical partners to ensure early communication of partner integration needs, schedule alignment, status on partner dependent development, to ensure partner alignment with all VA-BIT project schedules and critical partner integration points;
- Manage partner outage awareness and communication by ensuring partners are aware of schedule alignment, trigger dates, and due dates. Communicate partner outages and the impacts to VA-BIT systems up time and user satisfaction, perform resolution, corrective and preventive actions as necessary and notify stakeholders of actions completed and impact to systems;
- Manage data across environments including staging of data and data used for both scenario testing, validation and demonstrations;
- Communicate monthly- partner integration activities and partner list with current contact information in the Partner Coordination and Communication Plan. Partner information shall be updated monthly;
- Develop documentation and support processes in adherence with VA standards and stakeholder requirements to complete partner integration including change

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

requests, service requests, and web services change requests and National Service Desk (NSD) incidents;

- Support integration with partners, maintain integration guidelines, support System Oriented Architecture (SOA) and produce and consume services to support integration;
- Verify the project development schedule to partners and ensure that all schedules are aligned to account for system downtime and code promotion by managing and supporting partner integration dates, service dependencies, notification of issues and alarms and escalation and root cause analysis of service disruptions in all environments;
- Support demonstrations and coordinate environment setup for demonstrations and functionalities at the end of sprints;
- Support activities related to the VA RRR process including partner and stakeholder communication, partner deployment alignment, partner readiness;
- Maintain integration and provide subject matter expertise to ensure interfaces work with VA Self Service Portals, Chat/Co-Browse and KM software through VA Trusted Internet Connection (TIC), Virtual Private Network (VPN) or Citrix Access Gateway (CAG);

Deliverable:

- C. Partner Integration Strategy Plan
- D. Partner Coordination and Communication Plan

5.1.11.2.3 BUILD PLANNING

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance. Development builds shall be built in three (3) month cycles or less. The Contractor shall develop and deliver a Build Plan in collaboration with the project team prior to beginning the build. The Build Plan is the scope of work which will be completed in the agreed upon build timeframe. Each build will end with a new release or push to production, unless otherwise specified by the VA PM. Each build shall be delivered in 3-months or less and will be made up of the individual sprints conducted during the build. Each build will be fully tested by end users and will end in a new release candidate. The Build Plan must be completed prior to the start of the 3 month build timeframe. Conclusion of the Build Planning phase shall be defined per the agreements made with the VA PM during the Technical Kickoff Meeting. After the Build Plan is approved and the team is ready to start the build, the 3 month or less build cycle will start. Planning for future builds will occur during the execution of current builds.

The Contractor shall maintain the product backlog, continuously, for each build, in every release and throughout the life of the PoP within Rational Team Concert. All activity scheduled in each build and backlogs will be captured and have status showing all work

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

items, changes, impediments, and retrospectives. All data and artifacts in Team Concert shall be fully linked to requirements data and test data.

The Contractor shall:

- Schedule and facilitate backlog review, elaboration, and prioritization sessions with the VA PM, VA Product Owner and project team. This backlog grooming will occur continuously throughout the build to ensure the highest product priorities are being met. Meeting agendas, materials and minutes should be distributed per the VA PM's direction. During these backlog grooming sessions, the Contractor shall also:
 - Facilitate discussion and coordinate approval decisions of application defects, change requests, and elicit clarification of technical requirements, including assignment of priorities to defects and changes.
 - Update Rational based on the outcome of the change and configuration management processes. This includes revision of the functional and technical requirements and user stories in Rational Team Concert which shall be mapped to the existing requirements affected, creation of a ranked Product Backlog Report sorted by the priority agreed by the project team, and recording and managing new defects in Rational Team Concert.
- Facilitate selection of prioritized items from the product backlog to be included in the next build with direct input by the line of business and with approval by the VA PM. The approved items will be incorporated into a Build Plan for posting to Rational Team Concert.
- Conduct an Initial Design Review with stakeholders to ensure the design is technically feasible to be completed during the build.
- Provide support for identification of field sites, test environments, acceptance criteria, and ATO requirements.
- Develop, coordinate and validate Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU) and Service Level Agreements (SLAs) for partner dependencies that specifically highlight the commitment of partners to associated releases. The ISA specifies the technical and security requirement of the interconnection and the MOU defines the responsibilities of the participating organizations.

The Contractor shall provide a Build Test Plan to the VA PM for approval prior to initiating any development activities. This plan shall include both Contractor and VA testing activities, dependencies, and descriptions of the interfaces and interactions between solution components that are needed to test and validate. The Build Test Plan shall specify the types and scope of testing to be conducted during each product build (e.g. unit, functional, accessibility, system, reliability, usability, interoperability, regression, security, performance). The Contractor shall include testing related to non-functional requirements, (e.g. capacity, load, performance, installation, back-out, and rollback) in the Build Test Plan. The Contractor shall populate its Test Strategy section

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

of the Test Plan in VA's Rational Quality Manager tool within 15 days of the completion of the Build Plan.

At the conclusion of the Build Planning phase, the Contractor shall provide a Build Release Planning Package outlining the prioritized capabilities, estimation of size and timeline for completion.

Deliverable:

- E. Build Plan
- F. ISA/MOUs and SLAs
- G. Build Test Plan
- H. Build Release Planning Package

5.1.11.2.4 SPRINT PLANNING

The Contractor shall initiate Sprint Planning at the beginning of each sprint included in the build. All data and artifacts in Rational Team Concert shall be fully linked to requirements data and test data. The Contractor shall:

- In collaboration with the Business/Product Owner, take the approved prioritized, items identified from build planning and create and prioritize the sprint backlog;
- Identify user stories and tasks to be completed within the sprint, the agreement of acceptance criteria for the sprint, and readiness to begin sprint;
- Conduct a sprint design to understand what problem needs to be solved for each user story, understand critical business functions, test initial concepts, and look for objective feedback. Methods of design could include mock-ups, storyboards, and rapid prototyping;
- Update Rational to include any additional requirement elaboration details developed during this process;
- In collaboration with key VA Stakeholders, determine the testing events required for the Sprint;
- Update requirements traceability in Rational to demonstrate the linkage between what is in each sprint and the requirements;
- Create the Sprint Plan at the conclusion of the Sprint Planning. The Sprint Plan will be tailored to the scope of the sprint and will include sprint backlog, sprint design, sprint schedule, sprint acceptance criteria and sprint test events. The Sprint Plan shall be approved by the VA PM prior to the start of sprint execution.

Deliverables:

- I. Sprint Plan

5.1.11.2.5 SPRINT EXECUTION

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

The Contractor shall:

- Provide a certified Scrum Master to facilitate all ceremonies, ensure Rational is updated daily, enforce scrum framework, track and assist with removing impediments;
- Conduct sprint development including disciplined testing (unit, functional, regression) and reviews as a continuous process, to avoid finding issues at the end of sprint development. Develop the features and capabilities, including Source Code, as work items in Rational Team Concert that were established in the Sprint Plan;
- Initiate and conduct daily scrums (typically 15 minutes) to discuss the team's progress, impediments and daily plans;
- Attend Scrum of Scrums, which are half hour meetings, approximately three times per week, to discuss progress, impediments and cross-project dependencies with other projects;
- Provide Daily Rational Updates, to include progress on tasks during sprints, blockers and dependencies;
- Coordinate and support demonstration of the sprint activities and review/demonstrate acceptance criteria with the project team and key VA stakeholders at the end of each sprint;
- Obtain official Customer Acceptance of the Sprint;
- Initiate and facilitate a Sprint Retrospective at the end of the Sprint to capture team performance and lessons learned. Identify any planned sprint items not completed during the sprint, issues encountered and plans for resolution.

The Contractor shall document all activity executed during each sprint and update the backlog in Rational. This shall include all project artifacts such as work items, changes, risks, issues, impediments, and retrospectives. All data and artifacts in Rational Team Concert shall be fully linked to requirements data and test data. All project artifacts and source code will be under change and configuration management as outlined in the Configuration Management Plan

The Contractor shall deliver, at a minimum, the following Agile reports to show progress of development:

- Sprint Burn Down chart for each project/product being modified at the conclusion of each Sprint that illustrates the cumulative planned estimated metrics versus the cumulative actual completed metrics;
- The Velocity Chart showing the amount of value delivered in each sprint.

Deliverable:

- J. Sprint Burn Down and Velocity Charts

5.1.11.2.6 TESTING

The Contractor shall conduct sprint and build testing as follows:

Sprint Testing

The Contractor shall adopt Agile best practices for integration testing into each Agile development sprint and build. The Contractor shall conduct these tests as applicable throughout the development lifecycle using industry best practices of continuous integration methods and automated regression testing utilities approved in the One-VA TRM.

The Contractor shall provide a Test Plan in the Rational Quality Manager following the templates and data requirements for each test appropriate to each phase of development. The Contractor shall provide Test Results in the Rational Quality Manager which is the final piece of data that completes the Requirements Traceability Matrix (RTM). VA PM acceptance will occur through the Rational Quality Manager approval process.

The Contractor shall support security, accessibility, performance, technical standards, architectural compliance, user acceptance and initial operational capability tests, audits, and reviews. Security scanning is done by multiple methods and is done multiple times throughout the course of a project with methods such as infiltration testing, Web Application Security Assessment (WASA), code analysis tools (Fortify), etc. Accessibility reviews are performed through a variety of tool based and manual reviews, able to scan web applications and other technologies used for user interfaces. Performance testing is done through load testing and technical analysis of capacity planning data submitted by the project team. Architectural compliance assessments are done through submission of design materials to confirm compliance within the enterprise architecture.

The Contractor shall ensure all test and compliance review planning and execution details are included in the Test Plan. The testing and compliance results must be entered and maintained in Rational Quality Manager and under version control in Rational Team Concert. The Contractor shall ensure that results of all assessments of the project performed by the Contractor or by VA offices are consolidated into Rational for planning and status reporting.

When a defect is identified during testing, the Contractor shall log it in Rational, selecting the appropriate severity level. The Contractor shall provide sufficient information to recreate the defect for purposes of analysis and remediation. The Contractor shall prioritize the defect in the sprint backlog which shall be reviewed by the development team and approved by the VA PM. Based on the priority, the defect could be entered into the current sprint or entered into the backlog.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

The Contractor shall ensure Rational data is updated on a daily basis so VA stakeholders can access accurate and timely status.

Build Assembly and Testing

The Contractor shall assemble completed sprints into builds and test the overall build. The Contractor shall:

- Support test environment setup including setup, configuration, and data loading of the necessary development and test environments. The specific number of test environments that may be required shall depend upon the nature of the build.
- Support test events as required for each build including:
 - Product component testing
 - Component integration and system testing
 - Quality assurance testing
 - User functionality testing
 - Performance/load testing

The Contractor shall test during the Build phase and ensure the new sprint functionality work together in the event the build is determined to be a release candidate. The Contractor shall support all build testing events as required by the PM to explain functionality that was developed during the build, track defects found during build testing, and work with the PM to develop a plan to resolve defects discovered during build testing.

The Contractor shall complete the Section 508 Self-Certification Document. The Contractor shall support the VA Project Manager in obtaining the 508 compliance testing certifications for each enhancement that requires any change to user interfaces. Specific documents and information to be used to implement policies from the Section 508 Rehabilitation Act of 1973 and VA's Section 508 Accessibility Mandate can be found at <http://www.section508.va.gov/>.

The Contractor shall coordinate and conduct Test Readiness Reviews (TRRs) prior and Product Readiness Reviews (PRRs) with product demonstrations throughout the build, as defined by the VA Project Manager. The Contractor shall document and deliver to the VA PM the TRR and PRR review meeting results.

Following successful build testing, the Contractor shall make final, formal delivery of Final Development Code Files, Compiled Code, and supporting documentation.

The goal at the end of each build is to have a software package approved and production ready. However, every build may not be released into production. Multiple builds may be combined for release to production with the VA Business/Product Owner, VA project manager and COR approval.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Deliverables:

- K. Test Results
- L. Section 508 Self-Certification Document
- M. TRR/PRR review meeting results
- N. Final Development Code Files, Compiled Code and supporting documentation

5.1.11.2.7 ENTERPRISE SECURITY CHANGE CONTROL BOARD (ESCCB) AND NETWORK SECURITY OPERATIONS CENTER (NSOC)

All VA applications hosted in external environments requiring a connection to the VA network enter the VA intranet via a Business Partner Extranet (BPE). The VA BPE is a physically dedicated connection from the VA system to the external location that is exclusively for use by VA. The Contractor shall document, justify, and submit BPE configuration change requests to the ESCCB for approval. The ESCCB Technical Review process is intended to ensure that all proposed changes receive approval from all functional areas (Asset Management, Change Management, Enterprise Network Defense, Enterprise Operation, Service Design and Implementation) within VA-NSOC. Upon Approval of ESCCB Request by the VA, a VA NSOC NSD Help Desk Ticket will be opened to document the implementations actions associated with the approved request. All ESCCB requests prepared and submitted by the Contractor shall be included in the project schedule with sufficient time built into the schedule for the technical review, security review, approval, implementation, and testing process to complete (These requests average 2-3 per month).

The Contractor shall:

- Submit ESCCB requests during the requirements phase only when a project is required to interface with various backend systems that require changes to VA BPE;
- Provide an approved Platform level Interconnection Security Agreements (ISA) and supporting Memorandum of Understanding (MOU) for each new VA backend system, completed in accordance with VA Handbook 6500, Appendix D, Minimum Security Controls for VA Information Systems;
- Provide technical support to include verification testing, addressing any unanticipated issues encountered during implementation, and report the status during the required approved maintenance window between 1:00AM to 4:00AM EST for any follow-up actions that result from the review process;
- Complete the WASA checklist when VA applications hosted in an external environment require their application to be publically accessible on the Internet or if required by the Assessment & Authorization (A&A)/Authority to Operate (ATO) process. When this is the case, either a Privacy Threshold Analysis (PTA) or Privacy Impact Assessment (PIA) and WASA report will need to be attached to the ESCCB request. In addition, the WASA checklist includes a passing secure code review validation (e.g., Fortify scan result file) performed by the VA Information Security (OIS) Software Assurance (SwA) Program. Finally, the

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

WASA report also must address all Critical, High and Medium findings before the ESCCB request will be approved and implemented.

- Assist VA NSOC in any inquiry during the technical review within the ESCCB process.

Deliverables:

- O. Platform Level Interconnection Security Agreements (ISA) and supporting Memorandum of Understanding (MOU)
- P. Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA) Web Application Security Assessment (WASA) Report
- Q. Web Application Security Assessment (WASA) Report

5.1.11.2.8 SOLUTION TRAINING

The Contractor shall provide training of VA staff in the utilization and O&M of VA-BIT solution applications, components and services completion for each production development cycle for the duration of this TO. Training documents shall be provided for each release.

The Contractor shall:

- Provide a Help Desk Training Package for use by VA Help Desk personnel which consists of a system overview presentation, knowledge-based articles, and help desk troubleshooting procedures and instructions;
- Perform hands-on training with VA Help Desk personnel (not to exceed a total of 15 users) prior to the delivery of the VA-BIT solution for production. Provide minutes of training sessions to include a list of attendees, and time attended;
- Perform hands-on training with System Administrators/Operations staff (not to exceed a total of 15 users) prior to the delivery of the VA-BIT solution for production. Provide minutes of training session to include a list of attendees and time attended;
- Provide an End-User Training Package for use by end-users, (i.e., train-the-trainer), to include VA National Help Desk personnel, which consists of a End-User Training plan, Facilitator's Guide, Users Guide, PowerPoint slides, job aids and exercises;
- Perform on-site, hands-on training with designated application end-users (i.e., train-the-trainer), to include VA National Help Desk personnel, (not to exceed a total of 25 users) prior to pilot and national deployment roll-out of the VA-BIT solution for production. Training deliverables should be provided electronically, however, for the on-site, hands-on training sessions, hand-out copies of the Facilitator's Guide, Users Guide and PowerPoint slides are occasionally requested. In these cases, the Contractor is expected to print the hand-outs accordingly. Provide minutes of training session to include a list of attendees and time attended;
- Create and maintain a Developer's Guide;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Create and maintain On-line Help artifacts and scripts in a government hosted repository for Help Desk staff, ITC staff, and end-users;
- Support VIP Formal Product Documentation Reviews.

Deliverables:

- R. Help Desk Training Package and minutes
- S. End-User Training Package and minutes
- T. Developer's Guide
- U. Online Help Artifacts

5.2 VA-BIT PROCUREMENT DECISION MAKER (PDM) CAPABILITIES ON ON-PREMISE OR FEDRAMP-APPROVED CLOUD DEPLOYMENT (PHASE I)

VA-BIT shall be capable of leveraging the power of the Internet to aggregate data in real-time, then maximize it for relevancy for a broad base of users with the level of detail needed to make smart business decisions, quickly and decisively. VA users will be able to register in the VA-BIT portal, create an account, establish a userid and password, and receive notification of account approval or password reset via an approved VA email address. The VA-BIT shall automate integration and linkage of disparate data sources from both internal and external data sources. VA-BIT shall tie information together so that users can see what other contracting offices are buying within the agency, and which vendors they are purchasing from, at what prices. The Contractor shall provide the technical capability that integrates web services and Application Program Interface (API) from VA internal data sources or VA approved third-party data sources. The Contractor shall also create access to the data sources listed in this task via one or more APIs, web services solution (i.e., a software system designed to support interoperable machine-to-machine interaction over a network), or other relevant or useful Internet protocol (e.g., HTTPS). Batch downloading of data source shall be available but may not be the sole access; real-time, machine-readable access must be provided for all core data sources. Where applicable and available, core platform infrastructure and capabilities may be provided through third-party services or providers. Such providers must meet specific requirements for availability, reliability, and all Government requirements for security, terms of services, privacy, 508 compliance, etc.

The Contractor shall provide online user documentation detailing the minimum requirements for correctly using the Web API. The documentation shall minimally contain examples showing the correct syntax of API requests and their corresponding responses. The Contractor shall ensure that contact information for users seeking technical support is prominently displayed in the online Web API documentation. The Contractor shall develop a strategy for maintaining Web API versions over the life-cycle of the task order. The Contractor shall provide online, user-facing documentation that clearly distinguishes differences in usage between the current version of the Web API and its previous versions. The Contractor shall provide quarterly reports that list the number of times the Web API has been used.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Deliverable:

- A. Online Users Documentation for Web API
- B. Strategy for Maintaining Web API
- C. Quarterly Report on Web API usage

5.2.1 VA-BIT Standard Features

The VA-BIT portal will have the standard features:

- The VA-BIT portal will allow the user to set daily, weekly, or monthly alerts:
 - o Ability to receive Daily To Award Alerts in any region, VISN, or contracting office;
 - o Ability to track vendors receiving awards within and outside of the VA;
 - o Ability to track subcontractor awards;
 - o Receive Alerts on contracts by region, VISN, and contracting office for each prime contractor at the VA;
 - o Ability to track task orders, and an IDIQ to, with links to pertinent information;
 - o Receive a weekly spreadsheet for each of the standard reports for each bureau and contracting office within the VA;
 - o Receive alerts of new GAO Protests filings with links to daily FBO solicitations;
 - o Receive an alert when an agency awards a delivery/task order with details;
 - o Ability to configure keyword searches and set them to trigger automatic alerts;
 - o Receive alerts by specifying company headquarters location, place of performance, and narrow it down to any CBSA, state, county, or zipcode.
- All reports will have full drilldown capabilities to the company and to detail;
- Ability to name queries built with a custom name and save the search – to include all search parameters - according to that name. Display all saved searches in an easily identifiable, user-selectable list. Initiate search directly from the list without manual parameter entry;
 - Various search templates and filters provide the user with added functionality to look up a NAICS or PSF code;
 - Compound term processing shall allow users with appropriate permissions to input a requirement which can be automatically compared with vendor capabilities and other Government data sources such as FPDS.

Deliverable:

- A. VA-BIT Standard Features

5.2.2 AUTOMATED BACK-END DATABASE ATTRIBUTES

For Phase I, the Automated Back-end Database must possess the following attributes:

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- The database must be automated to drive the daily chain of events on the back-end;
- The database must trigger a call to specific structured and unstructured data;
- The database must be able to normalize the data before converting it to database consumable format;
- The database must have the ability to filter and categorize to funnel data into specific tables for fast access;
- The database must accomplish all events in one step ever needing to manually touch a single piece of data;
- The database must provide end users with up-to-date information on a daily basis.

Deliverable:

B. Automated Back-end Database

5.2.3 DATA SOURCES

At a minimum, the VA-BIT portal must integrate and link to the following external data sources:

- Federal Procurement Data System - Next Generation (FPDS-NG);
- Federal Business Opportunities (FBO);
- Grants.gov;
- Small Business Administration (SBA) Dynamic Small Business System (DSBS) ;
- General Accounting Office (GAO) Bid Protests;
- General Services Administration (GSA);
- Electronic Subcontracting Reporting System (eSRS);
- Small Business Administration (SBA);
- Federal Awardee Performance and Integrity Information System (FAPIIS);
- Past Performance Integrity Reporting System (PPIRS);
- Office of Management & Budget (OMB);
- Census.gov (for various secondary data sets);
- System for Award Management (SAM);
- Procurement Technical Assistance Centers (PTAC) contact information;
- USASpending.gov;
- Federal Assistance Award Data System (FAADS).

The VA-BIT portal must integrate data from the following internal data sources:

- Veterans Information Pages (VIP);
- Veterans Enterprise Management System (VEMS);

VA Electronic Contract Management System (eCMS) Forecast of Opportunities and Requirements Center for Excellence (FORCE)

Deliverable:

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- C.** Data integration and linking to external data sources
- D.** Data integration to VetBIZ/VIP/VEMS

5.2.4 FEDERAL BUSINESS OPPORTUNITIES REPOSITORY

VA-BIT shall contain a robust federal business opportunities repository of at least the last five years. VA-BIT shall have a powerful search capability that provides users the ability to search the synopsis text of any Request for Proposal (RFP) released during that period. VA-BIT shall provide direct access to all text contained within the attachments accompanied with many synopses of solicitations converting them into a form easy to process and analyze by the VA-BIT database application. VA-BIT shall support the capability to extract data and convert it to any format with relative ease. VA-BIT shall have search capability that provides users the ability search VA's Electronic Contract Management System (eCMS) solicitation documents to identify, and rank order findings based on relevance to program office's need statements. VA-BIT shall provide users the ability to search solicitation documents created across VA over the past five years, to include Performance Work Statements (PWS), evaluation criteria, Independent Government Cost Estimate (IGCE), and salient characteristics of the statement of needs. The VA-BIT solution shall also support the extraction and conversion of data stored in heterogeneous formats such as PDF, Word, Excel. VA-BIT shall provide an integrated ability to use Advanced Search capabilities to search across multiple data sources, such as Federal Business Opportunity (FBO), General Account Office (GAO) protests, Exhibit 53, FPDS-NG and description of awarded contracts, and tie it to programs and project identification numbers in OMB Exhibit 53.

At a minimum, the Federal Business Opportunities Repository should include the following features:

- Integration of FBO and FPDS-NG;
- Ability to view solicitations by contracting officer or contracting office, including industry sector, with link to FPDS transactions and award/solicitation documents, if available;
- Ability to view GAO protests with links to original solicitations, award notices, requirements documentation and FPDS-NG transactions;
- Ability to view responses submitted by a company when an award is announced in their favor from documents released on FedBizOpps;
- Custom search templates that allow you to save chosen criteria for receiving alerts;
- Configure and save unlimited keyword search parameters. Manage and edit searches from a custom link, or automate saved searches to receive alerts;
- Search for Exhibit 53 IT opportunities by project description, agency and/or investment type;
- Ability to view all solicitations posted daily in FedBizOpps, individually separated by document type, with links to original document attachments;
- Ability to view solicitations available dating back to Fiscal Year 2002;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Federal To Opportunities interlinked for cross-aggregation by Agency, Contracting Office, Zip Code, Posted Date, Classification Code, NAICS Code, Set-Aside, and linked to most GAO Protests and filings when possible;
- Agency summary sheet with the count of Request for Proposals (RFPs) linked to solicitation listings;
- Collaborative view for organization-wide tracking of each user-tracked solicitations;
- GAO Protest filings and complete Protest decisions linked to FedBizOpps, Company Profiles, made searchable by agency;
- Contacts and Email Addresses for VA Contracting Officers each linked individually to their name and the solicitation documents by type of RFPs released;
- A hyperlinked page showing all newly posted opportunities of the day for easy drilldown capabilities by agency, RFP type, Grants, and more.

Deliverable:

E. Federal Business Opportunities Repository

5.2.5 VA-BIT STANDARD REPORTS

At a minimum, the VA-BIT portal should have the following initial reporting capabilities presented in a dashboard format:

- Daily Reporting Suite: daily reporting of solicitation activity (pre-solicitation activity to include sources sought notices and request for information, solicitation amendments, combined synopsis/solicitations—and any revisions to the combined synopsis/solicitation, and special notices); reporting of daily dollars obligated versus year-to-date dollars obligated by contractor, agency/bureau, small businesses by spend, contracting offices, awards were the size determination by Contracting officer conflicts with the SBA Small Business size standards, and NAICS;
- Single-click access to reports featuring following data with drilldown capabilities:
 - Contracts by set-aside type;
 - Contracts awarded in last 30 days;
 - Contracts by NAICS and PSC codes;
 - Contracts by socioeconomic categories;
 - Contracts by Congressional District;
 - Contracts by type of competition;
 - FedBizOpps awards;
 - Contracts by Contracting office;
 - Contracts by socioeconomic program;
 - Contracts by place of performance;
 - Contracts roll-up by to number, aggregated with each individual transaction;
 - Expiring Contracts for all industry sectors, for any business type.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Industry overview by PSC and NAICS Codes with a dashboard view of the top 10 agencies, bureaus, prime contractors, competitive procedures (i.e., full and open competition, full and open competition after exclusion of sources (set-asides)), states, counties and fiscal year rankings within each industry for a specified time period;
- Tracking of Governmentwide Acquisition Contracts (GWAC)/Indefinite Delivery, Indefinite Quantity (IDIQ), and awards made against GSA schedules by NAICS, schedule type, category, company, SIN numbers, agency, SB versus OTSB, socioeconomic category, GWAC/IDIQ/GSA awards versus non-GWAC/IDIQ/GSA awards with drilldown capabilities for a specified time period;
- Report tracking sub to awards by NAICS; year-to-year comparison of sub to awards by agency, place of performance, state and NAICS; sub to awards by SBA District Office for a specified time period;
- Top OTSB by Cage Code, PSC, NAICS, funding code;
- Tracking of agencies activity by:
 - contact details of OSDDBU Staff; top administration officials, CIO and CFO with telephone, email, name and address;
 - agency organization chart; current year goaling report to track the status of an agencies small business goals;
 - top 10 organization within an agency ranked by dollars obligated and percentage of share;
 - top 10 prime contractors with drilldown capabilities to transactions and link to company profile;
 - top 10 contracting offices at the agency with drilldown;
 - top 10 small business prime contractors with drilldown capabilities and links to company profile;
 - top 10 subcontractors with drilldown capabilities and links to company profile;
 - top 10 GWACs by dollars obligated and percentage share;
 - top 10 congressional districts with names of congressmen and states;
 - top 10 competition categories with bar graphs for a specified time period;
 - top 10 IDV Contracts and names of contractors holding those Contracts ;
 - top 10 GSA schedule Contracts and contractors holding those Contracts;
 - top 10 NAICS codes by dollars obligated and percentage of share;
 - top 10 PSC industry codes by dollars obligated and percentage of share ;
 - top 10 first-time contractors in the federal government where specific agency was the awarding agency;
 - solicitation activity (pre-solicitation activity to include sources sought notices and request for information, solicitation amendments, combined synopsis/solicitations—and any revisions to the combined synopsis/solicitation, and special notices) by document type, nested by NAICS, showing comparison of YTD to the top agency issuing solicitations in each sector;
 - OMB Exhibit 300 tied to Contracts and Exhibit 53.
- VA goaling reporting suite for all agency components, VA agency sub-hierarchies down to Veterans Integrated Service Network (VISN) /Contracting Office level.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

This feature should include the rest of the government's agencies bureaus by major command (MAJCOM), Department of Defense Activity Address Code (DoDAAC), funding ID, office ID or other identification code for easy comparison purposes;

- FBO activity (pre-solicitation activity to include sources sought notices and request for information, solicitation amendments, combined synopsis/solicitations—and any revisions to the combined synopsis/solicitation, and special notices) by agency, place of performance, state, NAICS and type of set-aside;
- SBA Anomaly Report depicting where the contracting officer's size determination contradicts with SBA's size determination. Data will go back the previous 5 years. The following anomaly categories will be tracked:
 - SAM (to include any legacy Online Representations and Certifications (ORCA), and Central Contractor Registration (CCR)) record violations;
 - NAICS size standard violations;
 - 8(a) violations;
 - Hub-Zone violations;
 - DSBS NAICS size violations
 - SAM registration expirations;
 - OTSB coding miscues;
- Listing of expiring contracts by NAICS, Product Service Codes (PSCs) or Federal Supply Codes (FSCs);
- Simplified Acquisition Threshold (SAT) reporting suite with search filters, dollars and percentages of OTSB vs. SB dollars by agency under the SAT threshold

Deliverables:

- F.** Daily Reporting Suite
- G.** To Actions Summary Report
- H.** Industry Overview Report
- I.** GWAC/IDIQ Dashboard Report
- J.** Subcontracting Activity Report
- K.** Top OTSBs Activity Report
- L.** Agency Dashboard Report
- M.** VA Goaling Report
- N.** SBA Anomaly Report
- O.** FBO Activity Report
- P.** SAT Activity Report
- Q.** Expiring Contracts

5.2.6 VA-BIT SEARCH CAPABILITIES

At a minimum, the VA-BIT portal will allow the user to customize their search, save their search, and set alerts based on the results of their saved search. Additionally, the user will be able to upload a custom list of vendors and track award and de-obligation activity

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

of their custom list. The search results will be presented in a dashboard format to all the users to filter on the results for further analysis.

At a minimum, the user should be able to perform a search based on the following criteria:

- Company name;
- Company address;
- Business type (e.g., local government, minority-owned);
- Organization type (e.g., sole proprietorship, partnership);
- SIC;
- 8(a) entry/exit dates;
- Number of employees;
- Capabilities narrative;
- Current year revenue;
- Legal structure (e.g., Limited Liability Corporation, LLC);
- Fiscal year;
- DUNS number;
- Sector/agency/bureau;
- Awards based on IDIQ to vehicles versus those issued as standalone contracts;
- To base year;
- To expiration year;
- To amount;
- To action type (e.g., solicitation, modification);
- To type (e.g., Firm Fixed Price, Cost Plus Fixed Fee);
- Competitive procedures/extent competed (e.g. Full and open competition after exclusion of sources (small business set-aside), full and open competitions);
- Location (place of performance, CBSA, company headquarters, county, state, congressional district);
- Congressional District;
- Socioeconomic status;
- SAM registration date;
- Number of employees;
- Organization type (e.g., sole proprietorship, partnership);
- To Bundling;
- Solicitation Procedures (e.g., Simplified Acquisition Procedures, sealed bidding, contracting by negotiations);
- Contractors registered in System for Award Management;
- Country of Origin;
- Sub to Plan requirement;
- Sub to awards;
- Place of Manufacture;
- Multi-Year contracts;
- Price Evaluation Preference (e.g., HUBZone price evaluation);
- GSA Schedule Type;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- GWAC;
- Excluded parties;
- Number of offers received (Interested Parties);
- Contracts by PSC or NAICS or NAICS/PSC Combinations
- Categories other than full and open competition
- Application of labor laws (i.e., Service To Act, Davis-Bacon Act, Walsh-Healy Act), and Clinger Cohen Act;
- National interest (e.g., Operation Enduring Freedom, Hurricane Harvey).

Deliverable:

R. VA-BIT Search Capabilities

5.2.7 VA-BIT AUTOMATED QUESTIONNAIRE BASED RFI/SOURCES SOUGHT TOOL

VA-BIT portal shall enable users to conduct Request for Information (RFI)/Sources Sought rapidly and iteratively by establishing weighted questions, rapid replies with low level of effort from vendors and analytical engine that scores the results quickly.

Deliverable:

VA-BIT AUTOMATED QUESTIONNAIRE BASED RFI/SOURCES SOUGHT TOOL

5.2.8 VA GOALS MANAGEMENT DASHBOARD

The VA-BIT portal will have a robust goaling dashboard with specific focus on The VA Goals Management Dashboard is created with a specific focus on Veterans Affairs manageable spend as defined by the agency. The following features/capabilities will be incorporated into the VA Goals Management Dashboard:

- Graphical representation of Goaling for all six socio-economic categories;
 - graphs include the ability to toggle between monthly and cumulative performance compared to previous years and by component.
- Performance by socioeconomic category with the ability to drilldown to see historical spend;
- Tabular representation to allow user to view contractors included in that obligation amount;
- Goaling dashboard can be viewed by manageable spend, total spend and SAT spend;
- Ability to view spend by component, subcomponent, VISN and office, broken out by socioeconomic status;
- Comparison to VA total spend versus SAT spend;
- Drilldown capability to view to action, vendors, company profiles and individual transactions which comprise the manageable spend;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Graphical representation as well as data download capability to PDF
- Graphs can be viewed cumulatively or monthly;
- SAT Performance can be viewed by dollars obligated, actions and companies
- Additional links within dashboard to VA Analytic Tools to include (specific to VA spend):
 - VA taxonomy of categories;
 - Impact of modifications;
 - Anomaly reports by SBA office;
 - Top prime contractors;
 - Top small business prime contractors;
 - Top contracting offices;
 - NAICS/PSC industry reports;
 - Sub to award reports;
 - Geographic to analysis;
 - First-time prime contractors;
 - Top competition categories;
 - Top goaling category details;
 - Exhibit 53 IT initiatives;
 - Solicitations by document type;
 - Comparison of small vs. OTSB;
 - Socioeconomic analysis by SBA district;
- VA spend by to vehicle shows spending by IDV Vehicle types and tabular representation of GSA Schedule type and GWACs;
- Breakdown by FY, component, subcomponent, VISN and office;
- Further drilldown by socioeconomic status;
- Comparison of awards made to verified veteran owned business vs. non-verified veteran owned businesses shows contracts awarded by agency, both to verified and non-verified firms. Ability to filter result by socioeconomic categories and fiscal year. Results are displayed by \$ obligated, Number of Actions, Number of Firms and % set-aside;
- Contracts awarded to companies after date of denial shows contracts won by a company, after being denied a verified veteran owned business status. Ability to see results from FY 2011. View which agency(s) awarded the contracts, how much was awarded, across the number of actions and if a set-aside was used;
- Contracts awarded to companies after withdrawal date shows contracts won by a company after withdrawing their application from the verification process. Ability to see results from FY 2011. View which agency(s) awarded the contracts, how much was awarded, across the number of actions and if a set-aside was used;
- Ability to download to PDF and drilldown to specific vendor level detail on transactions;
- Link back to FPDS-NG and solicitation details/documents when available;
- VA Spend by NAICS Code shows spend by GSA Categories and by NAICS codes with the ability to link to contractors constituting that number;
- Ability to compare VA spend to total federal spend by dollars obligated, the number of actions and number of companies.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Deliverable:

S. VA Goals Management Dashboard

5.2.9 VA-BIT SIMPLIFIED ACQUISITION THRESHOLD (SAT) MANAGEMENT TOOL

The VA-BIT Portal will have a tool for VA Small Business Liaisons (SBLs) to track awards less than SAT (\$150,000) that may have been awarded to OTSBs.. The SAT management tool will have the following features/capabilities:

- Summary Report by large and small business with the ability to drill down to SB and non-SB contracts;
- Ability to exclude modifications (to include only base contracts), IDIQ and Federal Sources of Supply (FSS) contracts;
- View SAT contracts by component, subcomponent, VISN, office, GWAC, NAICS, GSA category, and FY and drill to actual transaction;
- View the dashboard with graphical performance, showing dollars obligated, number of companies and number of actions;
- See SB vs. OTSB analytics as well as further breakdown by socioeconomic status;
- SAT results page sorted by action obligation with ability to sort by other data columns;
- Links to company profiles as well as FPDS-NG transactions allowing SBL to perform analysis of to;
- Column for notes and action needed on SAT to using the following criteria:
 - CO Concurrence;
 - CO Non-concurrence;
 - Remedial;
 - Back for review;
- Ability to automatically save per user login;
- Ability to download a report at any time.

Deliverable:

T. SAT Management Tool

5.2.10 MARKET RESEARCH ANALYTICAL TOOL

The VA-BIT portal will have an integrated market research tool that can be used by individuals involved in any procurement effort to create market research projects on potential procurements from start to finish. The tool helps the user define the subject requirement based on customer need and helps create the market research report in a standard template that can be edited and saved. The portal allows the user to conduct comprehensive market research, automate potential searches for similar market research projects, and create the ability for users to reuse previously compiled reports

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

or portions thereof. Finally, the system will allow the user to forward for approval, create a PDF, and print a finished market research report for to officer review.

The market research analytical tool will pull existing data from the disparate data sources integrated within the VA-BIT portal to allow a user to obtain the correct data for the market research report. The tool should simplify the market research process by allowing the user to input market research data, view a vendor pool based on the input, flag verified VOSB/SDVOSB companies, view GWACs/IDIQs available for use and view a final report that can be saved, shared internally and printed.

The following are features within the market research analytical tool:

- Ability to input project details, including NAICS codes, estimated value, select a VA Portfolio pre-mapped to the VA's codes and Contracting Office code with budget identifier (any list values that are selected can be either dynamically created programmatically or can allow the user to enter as simple text);
- Author name and contact information auto-filled upon login into the VA-BIT portal;
- Ability for the user to select their organization within the VA;
- A market research objective template along with service descriptions so the user can use a standardized framework with suggested line of inquiry to complete it with maximum efficiency;
- Allow the user to select the place of performance by State, County, City or Zip, Core Based Statistical Area (CBSA), Metropolitan Statistical Area (MSA) as well as Contiguous United States (CONUS) and Outside the Continental United States (OCONUS);
- Ability to pull the top GWACs into the market research report based on user actions that precede it. This can be auto-generated based off portfolio/PSC as selected, as well as allow the user to research any known to vehicles that may be currently available for the procurement and add to the report manually;
- Text fields for users to input various answers on their way to complete the market research;
- Text boxes to explain the rationale for selections made, or add user known information to the template in case automation did not have it;
- Provide a question-based process for the user to navigate through the market research analytical tool;
- Text boxes that allow the user to add-in links to websites and existing reports within the VA-BIT portal;
- Ability to select if mandatory source requirements are needed;
- Populate potential supplier information which is automated based on the project details, requirements, service description and background. VA verified firms are clearly indicated. Ability to select or "add" supplier for final report. Quick link to company profile to verify supplier performance;
- A text edit block to enter comma-separated values. (e.g., entering keywords);
- Retrieve the next effective document based upon a filename search, date key name, or based upon to value;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- View Ability One companies that match the user-defined criteria;
- View a global directory of active vendors by socioeconomic status, especially those VA-verified SDVOSB and VOSB vendors;
- Company Profile allows user to look at awards history, contracting vehicles used across government, confirm if NAICS category is correct, SBA Size Standard verified, see if any protests filed by vendor, any FAPIIS indicators;
- Ability to view all saved projects and projects that are work in progress:
 - save market research reports;
 - share with other users of the VA-BIT portal;
 - print final market research report;
 - edit completed market research report;
 - edit other reports by users who have completed market research reports within the tool;
 - email the report to anyone outside the organization.

Deliverable:

U. Market Research Analytical Tool

5.2.11 FedRAMP-APPROVED CLOUD DEPLOYMENT

OSDBU intends to transition VA-BIT from a Commercially hosted Software As A Service (SaaS) solution to either an on premise VA Private, Community or Hybrid Cloud or a modern Federal Risk and Authorization Management Program (FedRAMP) certified Cloud Services with a VA Trusted Internet Connection (TIC) that support on-demand elastic resource management. The Software as a Service Solution must comply with the FedRAMP government program. Ensuring a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The new cloud service platform must allow for rapid, self-service onboarding of application development teams and Continuous Delivery using automation to deliver software products to Production. The VA-BIT solution must be available as Software as a Service (SaaS) with the flexibility of migration to an approved VA on premise or Cloud Hosting environment or a FedRamp approved host environment with a Trusted Internet Connection (TIC) to the VA. VA-BIT hosting infrastructure must be able to store and manage large amounts of structured and unstructured data from heterogeneous document formats with increased speed and power. Cloud Services must seamlessly integrated via single sign-on, and that improve business performance by providing OSDBU users with new and expanded capabilities that reflect, and are in keeping with, industry standards and best practices.

For the purposes of this requirement, this work PWS is focused on the six (6) central environments of the VA-BIT Cloud Hosting Solution: 1) Development, 2) Integration, 3)

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Pre-Production, 4) Quality Assurance, 5) Training and 6) Production. Features of the VA-BIT Cloud Hosting Solution physical architecture include:

- Scalability: All computer, processing, and storage components of the VA-BIT Cloud Hosting Solution's design can be scaled to accommodate an increase in the user counts. Blade servers can be quickly added to the existing chassis to provide the additional computing capacity that will be required to accommodate the additional users. VA-BIT Cloud Hosting Solution's Network Appliance storage solution controller heads are designed to handle the maximum amount of users specified for all supported environments.

Redundancy: VA-BIT Cloud Hosting Solution provides multiple levels of redundancy throughout the infrastructure. All of the critical network, server and storage components of the production environment have redundant pairs to ensure that the failure of one of the components does not result in a disaster recovery event being declared.

5.2.11.1 PROVIDE HOSTING CLOUD ENVIRONMENTS

Hosting services for each Application Environment consist of provisioning the six (6) central environments outlined below within 30 calendar days of a written request from VA. The Contractor shall provide a notification to the COR and corresponding PM when each environment is successfully completed.

- The Development Environment is used for Configuration, Customization, and Enhancement to develop Builds for release;
- The Integration Environment is used for COTS VA-BIT Configuration, Customization, Integration & Connectivity and Integration testing with systems, databases and mid-Tier data services;
- The QA Environment is used for User Acceptance Tests (UAT);
- The Pre-Production Environment is used for pre-production verification, build update/install verification and smoke testing. This environment will support VA-BIT performance testing using Production, Web-Services testing, and running performance monitoring tools and scripts. These performance testing capabilities shall be isolated from the development and production enclaves networking and storage files. Pre-Production environments will mirror production environments;
- The Training Environment will be used for training new users on the system as part of deployment and enhancements/new capabilities will be required for specific applications;
- The Production Environment is used for hosting of live veteran data that is accessed on a daily basis in the course of VA servicing of the Veteran and their beneficiaries. Production environments shall initially be classified as FISMA Moderate but shall have the option to increase that certifications classification to FISMA High at any point during the Period of Performance of this to upon notice from the Government.

For each Application Environment, the Contractor shall:

- Build all Application Computing Environments in accordance with Appendix A of this PWS;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Ensure that the hosting site being provided meets the requirements for Federal Information Security Managements Act (FISMA) at a Security Categorization of High by the kickoff meeting;
- Ensure the Hosted Cloud Environments meet the requirements of the Federal Information Security Managements Act (FISMA) at a Security Categorization of Moderate or High;
- Notify the VA PM of any planned maintenance, emergency maintenance, outages, or replacements of any equipment involved in the delivery of services for the purpose of awareness regardless of whether such activities impact the operational availability or performance of VA-BIT applications.
- Provide a secure access solution that allows VA-approved Systems Administrators, Database Administrators, and Security Administrators access to and control of the resources in the environments;
- Ensure that all resources involved in service delivery are properly and fully licensed, and maintain active vendor support. Upon award, the Government will provide a list of transferable software licenses to be used by the Contractor. The Contractor shall provide an accounting of current licensing and vendor support agreements for all resources that support the hosted environments. The list, which should include the expiration date for licenses, shall be updated quarterly and shall be included in the Bi-Weekly Status Reports;
- The Contractor is responsible for providing a solution necessary for scaling the environments to add additional capacity. The Contractor shall install and maintain the software and applications to support the required application environments.
- Provide interfaces to support portability and interoperability of applications in the Hosted Cloud Reference Appendix B for list of known interfaces. Additional interfaces with various VA enterprise services provider systems, several of which are discussed in section 1.0 Background, such as Identity and Assessment Management's (IAM) Master Veterans Index (MVI), Single Sign-On (VAAFI) and Access Services (AcS) systems; Customer Gateway Services (CGS) web data services; and Benefits Gateway Services (BGS) data services are crucial to VA-BIT's success;
- Use VA standard languages and tools (e.g., TRM). Reference <http://www.va.gov/TRM/TRMHomePage.asp> for current configuration;
- Support SSL encrypted transactions for Authenticated Chat and Co-Browse and secure messaging;
- Provide lower environments (Dev, INT, QA, training, pre-prod) in a private cloud sandbox that allow applications to be tested in the Hosted Cloud identically configured as the production system;
- Storage capacities - Provide VM shared storage with persistent, high availability, high performance (reference section 5.7.8 Service Level Agreement) shared storage and scalable to specified capacities for each environment;
- Provide both Standard performance storage and Premium performance storage to the capacities (reference section 5.7.8 Service Level Agreement);
- Provide updates to the Technology Roadmap that encompass technical refresh details. The Technology Roadmap shall document how the architected solution will 1) accommodate growth in application usage demands (just-in-time

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

scalability/growth in computing and/or storage capacity on demand, method for accommodating irregular surge requirements or unforeseen customer needs [e.g. increased application usage resulting from veterans inquiries surrounding Affordable Care Act open enrollment], enhancements to VA-BIT performance needs and requirements, etc.); 2) ensure continuity of service performance while adjusting to changes in government systems, regulations and/or requirements (evolving standards for disaster recovery, maturation of cloud computing security policies, assignment of FISMA High security categorizations, connecting to new VA IT systems as legacy systems are sun-setted and decommissioned, etc.); and 3) maintain competitiveness in hosting services provided to VA as technology evolves and improvements (cost competitiveness, technological parity [e.g. downtime, uptime, etc.], service speed and support, etc.);

- Provide a notification to the COR and corresponding PM when each VA-BIT environment is fully established and configured.

For each lower environment (Development, Integration, Quality Assurance, Pre-Production and Training), the Contractor shall provide all of the services detailed above and in the following sections:

- Section 5.1 – Program Management;
- Section 5.2.10.2 – Provide Network Connectivity;
- Section 5.2.10.4 – Hosted GFE Services;
- Section 5.5 -- Operations & Maintenance (O&M) with the exceptions of Emergency Incidence Response, SLA Requirements, Backup, Restore, and Disaster Recovery, and Hosted Cloud Environment Help Desk Support;
- Section 5.3.6.8 – Transition Support (Optional Task).

For each Production Environment the Contractor shall provide all of the services detailed above and in the following sections:

- Section 5.1 – Program Management;
- Section 5.3.2 – Provide Network Connectivity;
- Section 5.3.4 – Hosted GFE Services;
- Section 5.3.5 – Obtain and Maintain Authority to Operate (ATO);
- Section 5.3.6 – Operations & Maintenance (O&M);
- Section 5.3.6.7 – Data Calls and Reporting Requests;
- Section 5.3.6.8 – Transition Support (Optional Task).

Deliverable:

- A. Technology Roadmap Updates

5.2.11.2 PROVIDE NETWORK CONNECTIVITY

The Contractor shall have existing direct access to the VA Trusted Internet Connection (TIC) 2.0 Gateway Connection. Any deployment outside of the VA firewall is subject VA

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

TIC 2.0 Gateway Connection requirements in order to communicate with other VA systems within the VA Firewall. The Contractor must be able to meet integration with Active Directory via ADFS within thirty (30) calendar days and have experience with and knowledge of those policies.

The Contractor shall provide network solutions for connectivity between the primary and secondary site, subject to Federal Information Processing Standard (FIPS)-140-2 certification of equipment and configurations and the criteria set forth by the VA-BIT System Security Plan (SSP).

The Contractor shall deliver the following network functionality:

- Provide network connectivity that complies with FIPS 140-2, Section 1, Table 1, up to and including Security Level 3;
- Provide a redundant, secure encrypted network solution that provides connectivity between SITE1 and SITE2. This network solution shall meet the requirements of the applicable SLAs;
- Provide network connectivity to VA-provided circuits that use point-to point-IPsec Tunnels, with initial bandwidth of 10 Gbps. VA will provide access for communication to other VA business partners and mission oriented Internet based services thru the VA TIC 2.0 Gateway Connection. The Contractor's entry into the datacenter shall be a physically diverse path to mitigate any risk of a localized event disrupting communications;
 - Provide two connections to the WAN, through VA 2.0 TIC Gateway Connection via Business Partner Extranet (BPE) 1 providing sufficient bandwidth to meet all SLAs;
 - Provide two connections to the WAN, through VA 2.0 TIC Gateway Connection via (BPE) 2 providing sufficient bandwidth to meet all SLAs;
- Provide load balancing and firewall services inherently to the service as required by the specific security requirements that will each support at a minimum 100,000 simultaneous sessions;
- The Contractor solution shall support Internet Protocol Version 6 (IPv6) in accordance with the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>), August 2,2005_ <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>),and (<http://www.cybertelecom.org/dns/ipv6usg.htm>). IPv6 technology, in accordance with the USGv6: "Technical Infrastructure for IPv6 Adoption" (<http://www.nist.gov/itl/antd/usgv6.cfm>) and the NIST SP 800 series applicable compliance(<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support dual stack connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) shall support native IPv6 users, and all internal infrastructure and applications shall communicate using

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

Deliverables:

- B. SITE1 (Primary site) Network Configuration Diagrams
- C. SITE2 (Secondary site) Network Configuration Diagrams
- D. Updated SITE1 Network Configuration Diagrams
- E. Updated SITE2 Network Configuration Diagrams

5.2.11.3 DATA MIGRATION SOFTWARE AND SUPPORT

The Contractor shall provide, install, and maintain the Migration Software, which provides data adapters for data migration, data cleansing, and integration.

- The Contractor shall provide all required software, hardware, installation services, and configuration services required to facilitate use of data migration software. For informational purposes only, the Government is furnishing a listing of items that may be needed to facilitate the data migration software. This listing should not be considered to be comprehensive and exhaustive of all items needed to facilitate the data migration software. Additionally the Contractor may propose substitutions to the facilitation items that enhance the capabilities of the data migration software or increase the data migration software's capabilities and reduce cost. The Contractor shall provide all resources necessary (e.g. hardware) to enable use of data migration software;

Deliverable:

- F. Data Migration Software and Support

5.2.11.4 HOSTED GFE (HGFE) SERVICES

The Contractor shall provide the capability to host HGFE (reference Appendix E for sample listing of current security and performance monitoring equipment). VA will on occasion require physical servers and other ancillary equipment hosted at the Contractor's facility.

Specifically, the Contractor shall:

- Provide a secure space where VA can house HGFE (see Appendix B for sample specification details);
- Provide installation services for the HGFE into cabinets in standard (EIA-310-D) secure cage to which VA will have access. The Contractor shall be responsible

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

for receiving, unpacking, racking, cabling and connecting, powering and other tasks necessary to make the HGFE functional;

- Provide basic configuration of the HGFE per VA instruction to connect the HGFE to the designated environment per VA Staff instructions where they can be connected to one or more of the managed programs described in Section 5.3.1;
- Operate the HGFE and provide connectivity between the respective environments including any shared storage of the environments where the HGFE is hosted and other connection points as specified by VA within the standards specified in the SLA. (Note: Any given piece of HGFE will be considered operational after proper installation and successful connection meeting SLA requirements to designated devices in the environments or designated project);
- Permit access to the hosted HGFE for VA designated VA Staff;
- Provide disaster recovery for hosted services through a secondary site installation;
- Include accessible HGFE data in the backup rotation to support DR;
- Provide technical support via the Help Desk for the HGFE hosting environment but not the HGFE itself;
- Host communications HGFE in the environments with the physical separation required to mitigate any risk of a localized event disrupting communications.

Deliverable:

G. Hosted GFE Services

5.2.11.5 OBTAIN AND MAINTAIN AUTHORITY TO OPERATE (ATO)

The Contractor shall navigate the VA Office of Cyber Security (OCS) authority to operation (ATO) and ATO with conditions process, security process, scanning requirements, document preparation, etc. and shall provide a short thirty (30) calendar day transition plan to get the applications certified for at least ATO with conditions in that time frame.

The Contractor shall satisfy VA Directive 6500, Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. §§ 3541-3549), Office of Management and Budget (OMB) Circular A-130 and its appendices, The Privacy Act of 1974 (as amended) and the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publication (SP) guidance.

The Contractor shall ensure that the computing environments implement operational and security policies as required by a moderate system baseline according to NIST SP 800-53, Revision 4 VA shall identify the relevant inheritable security controls that must be implemented by the hosted computing facility and the Contractor shall ensure that the policies and controls are implemented immediately following to award. The Contractor shall be responsible for maintaining the documentation related to these controls and shall identify a Contractor representative who can act as a signatory

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

on security related deliverables such as the System Security Plan to attest to the implementation of the controls under the Contractor's controls.

The Contractor shall support audits regarding the implementation of these policies and assist in the collection and preparation of related compliance evidence. The Contractor shall retain and maintain referenced, applicable documents and deliverable documentation and make it available for review. The Contractor shall provide support to assist in meeting security requirements including:

- The Contractor shall be available for an interview and provide documentation or allow an onsite inspection for an Assessment and Authorization (A&A) audit;
- For any items that failed or demonstrated other than stratified controls identified by any auditing activity, the Contractor shall provide a Plan of Action and Milestones (POAM) addressing each issue noted in accordance with the failure classification levels: High, Medium, and Low. Contractor remediation shall follow the following schedule:
 - High = 60 calendar days;
 - Medium/Moderate = 90 calendar days;
 - Low = 120 calendar days;

Anything not remedied during the referenced timeframes must be escalated to the VA PM for further review. The Contractor shall be available for an interview, provide supporting documentation or allow an onsite inspection for POAM verification.

- The Contractor shall be available for an interview and provide documentation or allow an onsite inspection upon a mutually agreed schedule to validate its Security Test and Evaluation Plan for compliance with VA requirements;
- The Contractor shall conduct risk assessment of the Federal and private environments. Actions are to be documented on the POAM listing and reported to the VA PM;
- The Contractor shall allow for independent security controls assessment activities and scanning of any devices with prior notice;
- The Contractor shall provide copies of all policies and procedures and any other deliverables required to conduct a Security Controls Assessment at least 30 calendar days prior to the scheduled assessment;
The Contractor shall scan any non-dedicated device with a manual script run by Contractor staff and provide the scrubbed output to the government;
- The Contractor shall complete any FISMA Assessment related activities that are required;
- The Contractor shall, prior to the deployment of each VA-BIT Program application or major upgrade, perform the Assessment and Authorization (A&A) activities required to assure that addition of the application or major upgrade to the VA-BIT Program does not violate the conditions of the VA-BIT Program's Authority To Operate (ATO);
- The Contractor shall provide a report on the production environments Authority to Operate 60 calendar Days after to award;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- The Contractor shall support each VA-BIT application/tenant in the individual Assessment and Authorization process to include the initial establishment of an Authority to Operate and in any Continuous Monitoring after Authority to Operate is granted, which shall include all security controls, scans/reviews/remediation, documentation, and written plans to manage these controls.

Deliverables:

- H. Authority to Operate Transition Plan
- I. ATO Production Environments Report
- J. Plan of Actions and Milestones (POAM)

5.3 INTEGRATION INTO A THIRD-PARTY APPLICATIONS/WEB SERVICES/APPLICATION PROGRAMMING INTERFACES (APIs) (PHASE II)

The VA-BIT system will collaborate and integrate with a variety of systems and stakeholders and requires coordination and management of these partner engagements. The Contractor shall support partner management, coordination and integration efforts.

The Contractor shall:

- Develop a Partner Integration Strategy Plan on how the VA-BIT application can integrate with and consume services provided by partners, as well as share data with other VA applications per backlog requirements as part of the Partner Integration Plan. The Partner Integration Plan shall include an overview of the systems, a description of the major tasks involved in the integration of system components, the roles and responsibilities of integrating teams and organization, integration resources and the integration strategy that is to be supported;
- Coordinate integration and releasing activities to include dependencies with partner services, scheduling, and trigger dates;
- Collaborate with project partners, which may include other vendors, to establish the priority, scope, bounds, and resources and manage and mitigate project risks and issues regarding trigger dates and dependencies, blockers and proper escalation mechanisms;
- Coordinate and collaborate with integration partners on the development and execution of integration testing of all interfaces which shall occur in a partner integration environment that is configured by the Contractor and hosted by the 3rd Party Application's Cloud provider;
- Manage and coordinate touch points with critical partners to ensure early communication of partner integration needs, schedule alignment, status on partner dependent development, to ensure partner alignment with all VA-BIT project schedules and critical partner integration points;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Manage partner outage awareness and communication by ensuring partners are aware of schedule alignment, trigger dates, and due dates. Communicate partner outages and the impacts to VA-BIT systems up time and user satisfaction, perform resolution, corrective and preventive actions as necessary and notify stakeholders of actions completed and impact to systems;
- Manage data across environments including staging of data and data used for both scenario testing, validation and demonstrations;
- Communicate monthly- partner integration activities and partner list with current contact information in the Partner Coordination and Communication Plan. Partner information shall be updated monthly;
- Develop documentation and support processes in adherence with VA standards and stakeholder requirements to complete partner integration including change requests, service requests, and web services change requests and National Service Desk (NSD) incidents;
- Support integration with partners, maintain integration guidelines, support System Oriented Architecture (SOA) and produce and consume services to support integration;
- Verify the project development schedule to partners and ensure that all schedules are aligned to account for system downtime and code promotion by managing and supporting partner integration dates, service dependencies, notification of issues and alarms and escalation and root cause analysis of service disruptions in all environments;
- Support demonstrations and coordinate environment setup for demonstrations and functionalities at the end of sprints;
- Support activities related to the VA RRR process including partner and stakeholder communication, partner deployment alignment, partner readiness;
- Maintain integration and provide subject matter expertise to ensure interfaces work with VetBiz Portals, Chat/Co-Browse and KM software through VA Trusted Internet Connection (TIC), Virtual Private Network (VPN) or Citrix Access Gateway (CAG);

Deliverable:

- A. Partner Integration Strategy Plan
- B. Partner Coordination and Communication Plan

5.3.1 VA-BIT INTEGRATION TEAM

VA-BIT will be constantly evolving to meet VA priorities and may require continued integration across the platform throughout the PoP of this Task Order. VA may exercise this optional task for continued integration support. The integration team shall be responsible for planning and overseeing integrations across each task as well as developing reusable code components/web parts to be consumed by other applications. The Integration Team shall be capable of developing both web and non-web based interfaces with various VA systems and must be staffed sufficiently enough to accept work without schedule blocking. At a minimum, the Integration Team shall consist of at least five (5) dedicated members: a Project Manager or Technical Lead to run/oversee

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

the Integration Team, at least one (1) Architect possessing expertise with implementing the web-based applications one (1) Technical Analyst that can elaborate interface requirements as needed, and at least one (1) dedicated Developer. It is expected that Developers assigned to the individual development tasks will be required to provide input to the Integration Team on a regular basis. This task may be exercised a single time per option period. The PoP of the optional task shall coincide with the PoP of the option period in which it is exercised.

Deliverable:

C. Reusable code components/web parts

5.4 DEVELOPMENT OF VENDOR CAPABILITIES (OPTIONAL TASK) – (PHASE III)

The Contractor may be responsible for developing vendor-facing capabilities within the VA-BIT solution. The vendor (external end-user) will be able to create a profile, search opportunities, create a customized search based on user-defined criteria, save their search, set alerts based on the results of their saved search, view upcoming procurement events (e.g., Industry Days, OSDBU Direct Access Program events), set reminders for upcoming events, and other activities to help external end-users gain access to upcoming VA opportunities. Additionally, VA (internal) end-users will be able to search profiles established by the external end-users to aid them in conducting market research.

5.4.1 VA-BIT VENDOR DASHBOARD FEATURES

- Upon logging into the vendor dashboard, the user is presented with several features laid out in a convenient format for easy access to important portals & features.
 - Dashboard at a glance (Tiles)
 - Add Events : Provides the user the option to add Direct Access Events
 - Percentage of Profile Completed: Clicking on “Update” allows the vendor to make edits/updates to their profile
 - Opportunities: View opportunities posted by PDM’s
 - Users have access to different features located in the Navigation Bar.
 - Events: Access & view “Upcoming Events” “View past Events”
 - Navigation: Profile will consist of the following:
 - “View My Profile”
 - “Edit Profile”
 - “Manage Files”
 - “Add/Update Categories”
 - “Change Password”

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- “Notification Center”
- “Global Directory” allows users to
- search other participants & verify
- participation in the National
- Veterans Small Business Engagement
- “Opportunities” allows the user to
- view which opportunities matches
- their profile & allows searching
- opportunities posted by PDM’s
- “Logout” allows the user to securely
- exit their dashboard
- FAQs
- Support page with manual, tutorials & webinars
- Users have access for profile information in two sections (on the front of the main user dashboard, & the Navigation Bar). Users have the ability to edit & view profile information:
 - Profile Completed/Update
 - Quick stat of profile completion
 - Quick link to update profile information
 - Profile (Navigation Bar)
 - “View Profile” information
 - “Edit profile”
 - Manage important documents/logos
 - “Add/update Business Categories”
 - Change/update user password
 - View any event notification
 - Such as time changes, meeting cancellations, and new opportunities posted.
- Users have the ability to access & view their potential matches/opportunities on the Navigation Bar.
 - Opportunities: This module allows Vendors to view all the PDM Opportunities that matches the service & products the Vendor provides, and View the Compatibility Score for the Opportunity posted
- In addition to the quick links located in the three main boxes, users have access to many different features located in the “Navigation Bar”. This section is divided into three main categories: Events, Navigation, & Support.
 - Events
 - Access & view upcoming events
 - View past event
 - Navigation
 - Dashboard brings users to the screen you see initially at login Profile allows user to access different aspects of their profile:

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- “View my Profile”
 - “Edit Profile”
 - “Manage Files”
 - “Add/update categories”
 - “Change Password”
 - “Notification Center”
- “Global Directory” allows users to access all the participants for VA BIT “Opportunities” allows the user to explore opportunities posted by PDM’s
- “Logout” allows users to exit their profile & return to the event/portal page
- “FAQ” grants users to access support pages & tutorials
 - Support sends users to the support page
 - Access tutorials & webinars regarding main features of the user dashboard
- Under “View Profile”, Vendors have the ability to view their profile the way a PDM would. The user can then review their information for accuracy:
 - Click on “View Profile”
 - General Information tab
 - “Upload capability statement”
 - View general posted information
 - Participating Events tab
 - Verify if the participant is attending the National Veterans Small Business Engagement
 - Business Categories tab
 - View business categories
- Under “Edit Profile”, users have the ability to make changes, or add additional information at their convenience. The system will automatically highlight any blank fields that are necessary for 100% completion of the profile. “Edit Profile” is divided up into 5 different sections: Company/Organization, Business Information, Point of Contact's, & Company Data.
 - Company/Organization Information
 - Business Information
 - Point of Contact
 - Company Data
- Searchable formatted capabilities statements, that draws to maximum extent possible from existing government and third party data sets.
- Users have access to upload capability statement, company logo, and brochure to help advance their profile to potential PDM’s. Files must be formatted into a GIF, JPG, PNG, & PDF, DOC, and DOCX. Files may not exceed 10M limitation.
- Click on “Manage Files”
 - Upload Logo
 - Allowed formats - gif jpg png
 - Max resolution -

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- 1600x1600px
 - Max size - 5M
- Upload Brochure
 - Allowed formats – pdf
 - Max size – 10M
- Attendee Photo
 - Allowed formats –jpg jpeg png bmp gif
 - Max size - 10M
- Locate the “Attach File” button for each section.
- Users are provided with access to edit, add & remove business categories. The user is also presented with useful “How to” tips to help post business categories.
 - Click on “Add/Update Categories”
 - Tips for Business Categories
 - Select Business Categories
 - PDF link to view business categories
 - Add your business categories tool
- Once the user has completed the initial registration process they have the ability to change/update their current password.
 - Click on “Change Password”
 - Enter current password
 - Enter new password
 - Retype new password
 - “Save” or “Cancel”
- The notification center gives users a full legend (listing providing information on each notification in relation to importance of completed task). The notifications specify the type, device, date/time created, message, & option for action taken.
 - Click on “Notification Center”
 - Legend
 - Action “Success” notated in green
 - Action “Information” notated in blue
 - Action “Notice/Warning” notated in yellow
 - Action “Alert” notated in red
 - Notification & designated fields
 - Type
 - Device
 - Date & time created
 - Message
 - Action
 - “View Details”: Allows users to view details specified by the notification.
- Under the “Opportunities” tab users can manage potential matches, filter out buyers, utilize a search function, view compatibility score, view opportunity details & view organization details.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Click on “Opportunities”
 - Recommended Matched Opportunities: Displays the total number of matches
 - “Add Filters”: Allows users to apply search criteria on business matches.
 - Compatibility Score: View requirements met & not met
 - Click on opportunity name to reveal opportunity details
 - “View Organization Details
- The “Add Filters” function allows users to filter out matches based on set criteria’s, compatibility score, & business categories.
- Click on “Add Filters”
 - Compatibility score: Apply filter based on user’s compatibility score from 1 to 100 in relation to PDM posted opportunities
 - Business Categories: Filter out opportunities based on Vendor business categories
 - Categories in the filter are determined by the categories in the user profile
 - “Add” or “Close” filters to apply selections or disregard
- Users have access to other upcoming events under “Add Events” tile. With this features users can locate Direct Access Events
 - Event Search function: Timeline of Direct Access Events
- Users have the ability to generate a compatibility score for a vendor or multiple vendors based on an algorithm or set of algorithms. The compatibility score tool shall enable Program Offices and other decisions makers to quickly identify and weight the characteristics of a vendor that are important to them, searches vendor data, and assigns a compatibility score for vendors based on weighted factors. This tool should be linked to other tools that address vendor characteristics
 - Compatibility attributes (not all inclusive):
 - VOSB Verified
 - Federal Supply Schedule
 - Revenue
 - Facility Clearance
 - DCAA Compliant
 - Number of Prime Contracts
 - Business Certification
 - Mentor/Protégé
 - Socio Economic Category
 - Years in Business
 - Past Performance
 - Non-government performance
 - Number of Employees
 - Number of Veteran employees

5.4.2 VA-BIT COMPATIBILITY MATCHING TOOL:

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- VA-BIT shall provide Program Offices/Program Managers/Contracting Officers/Other designated personnel the ability to generate a compatibility score for a vendor or multiple vendors based on an algorithm or set of algorithms. The compatibility score tool shall enable Program Offices and other decisions makers to quickly identify and weight the characteristics of a vendor that are important to them, searches vendor data, and assigns a compatibility score for vendors based on weighted factors. This tool should be linked to other tools that address vendor characteristics
 - Compatibility attributes (not all inclusive):
 - VOSB Verified
 - Federal Supply Schedule
 - Revenue
 - Facility Clearance
 - DCAA Compliant
 - Number of Prime Contracts
 - Business Certification
 - Mentor/Protégé
 - Socio Economic Category
 - Years in Business
 - Past Performance
 - Non-government performance
 - Number of Employees
 - Number of Veteran employees

5.4.3 VA-BIT PAST PERFORMANCE TOOL:

- VA-BIT shall provide Program Offices/Program Managers/Contracting Officers/Other designated personnel a tool that draws data from PPIRS/CPARS and PPQ to provide PM with past performance information for Market Research Reports.

5.4.4 VA-BIT ORGANIZATION RISK TOOL:

- VA-BIT shall provide Program Offices/Program Managers/Contracting Officers/Other designated personnel a tool that draws on commercial data bases to identify organizational, legal, financial risks associated with a vendor.

5.4.5 VA-BIT RESPONSIBILITY COMPETENCY TOOL:

- VA-BIT shall provide Program Offices/Program Managers/Contracting Officers/Other designated personnel a tool that identifies the elements of the Statement of Responsibility and Certificate of Competency and pulls information from various data sets to fulfill the requirements of those actions to maximum

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

extent possible, while minimizing the need to request additional information from vendor.

5.4.6 RELEASE AND DEPLOYMENT

5.4.6.1 PRE-RELEASE SUPPORT

The VIP Release Process is conducted during the build and development cycle by one or more assigned Release Agents, who perform frequent, regular reviews of required and appropriately linked product data in the mandated repositories. The Release Agents also provide timely feedback to the product team concerning the status of the product data and the status of the team's compliance with the VIP Release Process. The Contractor shall support OI&T's single VIP Release process.

The POLARIS calendaring process and tool will be used to track software installations, hardware replacements, system upgrades, patch releases and implementations, special works in progress, and other deployments in any VA production environment. The Contractor shall provide data for populating and updating the POLARIS calendaring process for each release and deployment.

The Contractor shall work with the PM and stakeholders to develop a Build Release Package that will outline processes and documentation needed to deploy the build.

To complete the Build Release Package, the Contractor shall:

- Develop/update/finalize the Platform level Production Operations Manual (POM) and/or the Technical Manual, depending on the product being produced. The POM or Technical Manual shall include regular maintenance and operations information, Responsibility, Accountability, Consulted, and Informed (RACI) information, process flowcharts, dataflow diagrams, key monitoring indicators, and troubleshooting information;
- Develop the User Guide, which addresses procedural information for the business users on daily operational use of the software;
- Hold test site calls with VA staff to include Release Coordinators and VIP Release Agents once the product is approved for IOC production testing;
- Develop and maintain the Version Description Document (VDD) which is used to identify, maintain, enhance, and recreate the product (IT asset) throughout its lifecycle;
- Create a Transition Plan to include a transition meeting to present a coherent methodology for transferring responsibility for system sustainment to the desired sustaining organization. The Contractor shall describe the system components, architecture, interfaces, and environments and then clearly articulate what elements are to be transitioned to the sustaining organization;
- Develop a Deployment and Installation Guide to include back-out and rollback procedures, a listing of any changes to Security Keys that impact an end user's

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

ability to access and perform a system function, Technical Manual, System Security Guide, System Contingency Plans, and Disaster Recovery Plan in accordance with VIP, ProPath and Release requirements;

- Provide all documentation required to obtain/maintain an Authority to Operate (ATO) as specified in the EPMO Website;
- Ensure each Build's final source code is appropriately stored in Rational Tools

Deliverable:

V. Build Release Package

5.4.6.2 INITIAL OPERATING CAPABILITY (IOC) SUPPORT

An Initial Operating Capability (IOC) Evaluation is a limited production release that is required for all system solutions that will be released to multiple locations, such as a VistA release. The Contractor shall correspond with the project's VA Release Agent to confirm whether the IOC approval process is required. The evaluation occurs after all testing has been completed and user acceptance has been granted. If deemed necessary by the VA Release Agent, the Contractor shall observe and support IOC by assisting with the tracking and investigation of issues and remediation of defects as needed.

The Contractor shall support a 10 day error free (no identified Severity Level 1 or 2 defects) IOC in the production account. The Contractor shall resolve and track all defects and document the findings in the Defect/Fix Status Report, as well as address all issues and questions identified during IOC. For each defect identified, the Contractor shall log the defect, identify a resolution for the defect, and provide a Defect Resolution Plan, including timeline and impacts to the schedule, software code and documentation. Following VA PM approval of the plan, the Contractor shall execute the approved plan. At the completion of each defect correction, the Contractor shall update the software source code and compiled code, coordinate the installation of the software update into the test site production accounts, and deliver updated supporting documentation as identified in the below paragraph.

After any defect correction during IOC, IOC shall continue with the updated software source code for a minimum of five business days error free before exiting IOC.

The Contractor shall support IOC evaluation activities (if confirmed by the VA Release Agent that they are indeed required) to ensure IOC entry and exit criteria are met. The Contractor shall support installation and configuration at VA test sites, and support identification and development of remediation plans for defects as required.

Deliverables:

- W.** Defect/Fix Status Report
- X.** Defect Resolution Plan

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Y. Updates to Software Source Code, Compiled Code and Supporting Documentation

5.4.6.3 RELEASE AND DEPLOYMENT SUPPORT

In accordance with the VIP Guide, release and deployment support begins upon successful completion of Production Deployment for the first release.

Following successful completion of the IOC, the Contractor shall update and finalize a Technical Documentation Package, including updates to the existing System Design Document, materials, manuals, user guides, and release notes and make a final, formal delivery to VA. If any discrepancies are found, the Contractor shall be responsible for resolution. The Contractor shall also update and finalize the software source code and make a final, formal delivery to VA.

Successful completion of deployment requires that the solution or application has received the required approvals and authorizations. The Contractor shall adhere to all applicable policies and procedures to enhance the VA-BIT applications and ensure that the architecture is in accordance with VA's architecture guidelines.

The Contractor shall provide support and coordinate each release with the VA technical staff and the development and integration teams of the systems that are interfaced, and resolve issues and ensure that migration is completed as planned to the proper technical environments.

The Contractor shall:

- Support all VA-BIT System enhancement deployments;
- Work in conjunction with VA to provide deployment support for each of the scheduled releases;
- Participate in coordination activities to review deployment requirements and verify the sufficiency of deployment plans and checklists.

In conjunction with the VA PM and stakeholders, the Contractor shall produce a Release and Deployment Support Plan to outline the implementation, deployment, training, and transition of the application to the maintenance team. The Contractor shall include release instructions, design documents, and maintenance instructions for the solution. Instructions shall include all specific steps for installation of the software and also a "Rollback" procedure that can be used in the event of a problem. The Release and Deployment Support Plan shall outline how the Contractor will accomplish this task. The Release and Deployment Support Package shall include updated and final technical documentation reflecting any changes occurring during IOC:

- Solution Deployment Packages (SDP) with smart scripting to VA in support of project deployment efforts. The SDP shall include all applicable required Artifacts

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

covering the Release Management, Product Documentation, and Product Support phases;

- Updated Platform level Production Operations Manual and the Deployment, Installation, Rollback, and Back-out Guide for quick diagnosis of operational problems. The Contractor shall also develop a Deployment Guide with instructions on how to deploy each component, inclusive of component relationship diagrams;
- Updated Technical Documentation Package;
- Technical Manual within the Release Package that will document the technical design, interactions with other systems, and configuration in the VA Software Library to address changes resulting from an enhancement;
- Updated Business Release Notes within the Release Package that describe changes to existing software and new features and functions created as a result of this enhancement;
- Close coordination with the VA Release Agent is required to ensure that Production Releases meet certain standards for successful deployment.

Deliverables:

Z. Release and Deployment Support Plan and Package

AA. Technical Documentation Package

BB. Final Software Source Code

5.5 ADDITIONAL VA-BIT DEVELOPMENT (OPTIONAL TASK 2)

VA-BIT will continue to evolve to meet VA priorities and may require completion of additional projects throughout the PoP of this TO. VA may exercise this optional task for additional scrum teams to support development of VA-BIT projects following the software development lifecycle described in Section 5.2, including all subparagraphs, of this PWS. The specific scope of functionality to be delivered for each build in the optional task will be determined with VA Product/Project business owners prior to the start of each build cycle based on current business priorities. The Contractor shall provide an additional scrum team made up of the appropriate technical skill sets to support multiple builds throughout each PoP. Each Scrum Team shall include at least one resource with expertise and experience with implementing the web-based applications. Each Scrum Team shall also include a dedicated resource that is capable of elaborating complex requirements. A Certified Scrum Master is recommended per team; however, Certified Scrum Masters may be shared across two when appropriate size and technical leadership is available. The Contractor shall provide development management resources to support each release cycle, to include defect management following the release of all software into production. This optional task may be exercised anytime in the base period and/or the option periods.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

5.5.1.1 WARRANTY SUPPORT

For a period of 90 days after the final Deployment release is completed, the Contractor shall warrant all requirements and deliverables in the scope of this contract. Defects may be identified by the Government and its designees, to include all necessary personnel as designated by the COR. For each defect identified, the Contractor shall triage the defect in accordance with the table below, identify a resolution for the defect, and provide a plan for resolution, including timeline and impacts to the code and updates to Rational. Following COR approval of the Contractor defect resolution plan, the Contractor shall execute the approved plan.

TABLE 1: RESPONSE TIMES FOR TIER 2 AND TIER 3

Severity Code	Tier 2 Initial Response to Customer	Tier 2 escalates to Tier 3 for initial contact	Tier 3 response to Tier 2 Tier	Tier 2 requests updates from Tier 3 based on SLA resolution	Resolution Time based on SLA from time incident initially reported
1 – Critical	15 minutes	0-15 minutes	15 minutes	On call until issue resolved or hourly status check	0-2 business hours
2 – Serious	1 hour	30 minutes	1 hour	On call until issue resolved or hourly status check	2-4 business hours
3 – Moderate	4 hours	1 hour	4 hours	Daily	4-8 business hours

5.5.2 OPERATIONS AND MAINTENANCE SUPPORT

System solution operation and maintenance (O&M) support activities are related to the on-going support for the performance of routine, preventive, predictive, scheduled, and unscheduled actions aimed at maintaining the system performance by supporting the

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

application from desktop to server, real time monitoring system performance metrics, and coordinating with other VA and non-VA systems. This includes performance monitoring and bug fixes, and preventing system/production failure by working with the hosting and development staff to properly size and deploy capabilities to support performance. In addition, O&M support activities include correcting production software defects with the goal of increasing efficiency and reliability on a continuous basis via bug fix/hotfix releases and deploying patches/upgrades as needed.

In support of these activities, the Contractor shall configure, develop, maintain, test, and deploy VA-BIT maintenance releases and/or bug fix/hotfix releases applying the same life cycle tasks, as applicable, described in Section 5.2. The Contractor shall provide technical documentation and execute these life cycle processes throughout the period of performance to support the delivery of VA-BIT functionality. Releases may occur after hours and/or on during the weekend. It is expected that all deployment release packages are completely developed and SME advisory and troubleshooting support is provided. For Production releases, Contractor support staff shall be identified and available if there is a problem.

The Contractor should deliver a report on recommended future improvements to the VA-BIT portal.

5.5.3 OPERATIONS AND MAINTENANCE SUPPORT (OPTION PERIODS ONLY)

System solution operation and maintenance (O&M) support activities are related to the on-going support for the performance of routine, preventive, predictive, scheduled, and unscheduled actions aimed at maintaining the system performance by supporting the application from desktop to server, real time monitoring system performance metrics, and coordinating with other VA and non-VA systems. This includes performance monitoring and bug fixes, and preventing system/production failure by working with the hosting and development staff to properly size and deploy capabilities to support performance. In addition, O&M support activities include correcting production software defects with the goal of increasing efficiency and reliability on a continuous basis via bug fix/hotfix releases and deploying patches/upgrades as needed.

In support of these activities, the Contractor shall configure, develop, maintain, test, and deploy maintenance releases and/or bug fix/hotfix releases applying the same life cycle tasks, as applicable, described in Section 5.2. The Contractor shall provide technical documentation and execute these life cycle processes throughout the period of performance to support the delivery of VA-BIT functionality. Releases may occur after hours and/or on during the weekend. It is expected that all deployment release packages are completely developed and SME advisory and troubleshooting support is provided. For Production releases, Contractor support staff shall be identified and available if there is a problem.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

I

The below table depicts the applicability of required O&M support

	HIGH
Change and Configuration Management Support	X
Application Support/End User Management	X
Maintenance Release Deployment Management	X
Database Migration Support	X
Operational Support	X
Service Desk Support	X
Testing Support	X
Technical Subject Matter Expert (SME) Support	X
Tech Refresh	X
COTS Software Patches	X

During Option Period 1, if exercised, O&M support of VA-BIT shall commence on June 30, 2018 and run through the end of the Option Period 1 PoP. O&M support during Option Periods 2 and 3, if exercised, will commence immediately after expiration of the prior Option Period. The base requirements of the Option Periods only include O&M support for Core applications. Should O&M support of non-Core applications be required, the appropriate optional task(s) will be exercised.

5.5.4 CHANGE AND CONFIGURATION MANAGEMENT SUPPORT

Change and Configuration Management addresses the governance, process, roles, and responsibilities for the intake, disposition, and documentation of configuration and/or code changes under the direction of VA in support of applications that have been deployed to production.

The Contractor shall:

- Update the existing Change and Configuration Management Plan;
- Perform technical analysis to include: identifying dependencies on other tasks; estimating the level of effort to address defects and change requests; assessing the impact of changes on the existing system; and classifying changes as indicated below:
 - Corrective Sustainment which is the diagnosis and correction of program errors after software release;
 - Adaptive Sustainment which is the modification of software to interface with a changing environment or congressional mandates;
 - Preventive Sustainment which is the modification of software to improve future maintainability or reliability as a result of a requirement to perform a hardware re-platform or operating system/system software upgrade;
 - Perfective Sustainment which is the modification of the software to improve future functionality based on best practice recommended by the Subject Matter Experts (SMEs), sustainment staff and business. This shall

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

include software patches, code optimization and incorporation of upgraded and effective software or plugins to improve performance and usability.

- Schedule Change Control Board (CCB) meetings, prepare agendas and distribute meeting materials under the COR and VA Product Owner's direction. During these meetings, the Contractor shall:
 - Facilitate discussion and coordinate approval decisions of application defects, change requests, and elicit clarification of technical requirements, including assignment of priorities to defects and changes;
 - Distribute draft CCB meeting minutes, receive and incorporate comments, and distribute a final version of the meeting minutes;
- Update Rational Team Concert (RTC) based on the outcome of change and configuration management processes. This shall include:
 - Revision of the functional and technical requirements and user stories in RTC which shall be mapped to the existing requirements affected;
 - Creation of a ranked Product Backlog Report sorted by the priority assigned by the CCB;
 - Record and manage new defects in RTC.

Deliverables:

- A. Updated Change and Configuration Management Plan
- B. Ranked Product Backlog Report

5.5.5 APPLICATION SUPPORT/END USER MANAGEMENT

The Contractor shall:

- Create, retrieve/reset, update, and delete user accounts and profiles; provide maintenance support including managing Business units and Teams where applicable.
- Provide a VA-BIT Users List Report, utilizing current user lists, to VA of all active and deactivated Users as changes are made;
- Manage all VA-BIT users and credentials in the production related VA-BIT environments including integration, QA, training, pre-prod and production.

Deliverable:

- C. VA-BIT Users List Report

5.5.6 MAINTENANCE RELEASE DEPLOYMENT MANAGEMENT

Maintenance Release Deployment refers to all of the activities that support the promotion of developed functionality, after User Acceptance Testing (UAT), from a lower level environment (i.e., Quality Assurance, Integration, Pre-Production, etc.) to the Production environment as defined in section 5.2, in close coordination with the VA-BIT

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Hosting provider and Developer as necessary. For the Option Periods, if exercised, this support shall be provided for all these environments as well as the training environment. The Contractor shall provide maintenance and release deployment management and support for the applications in production and ensure completion of all the tasks and deliverables detailed in Section 5.2.3 (Release and Deployment Package) for each release as needed, following guidance from a VA Release Agent. The Contractor shall also provide USD support where applicable. Releases shall occur as specified in the resolution requirements within the Severity Levels table in section 5.5.8.

5.5.7 DATABASE ADMINISTRATION SUPPORT

The Contractor shall provide database administration for VA-BIT . As part of database administration support, the Contractor shall:

- Install, manage, and maintain database service instances
- Create new database for the production environments;
- Perform daily backup and restore databases as required;
- Create database-level accounts needed for VA Organizations;
- Manage database permissions;
- Troubleshoot back-end database issues;
- Document bug and errors in RTC and provide Bug and Error Reports and remediate as necessary;
- Ensure proper database licensing is applied to the VA-BIT instances;
- Support, configure and administer Database Server Reporting Services;
- Support, administer and configure KM and Chat & Co-Browse databases and file servers;
- Upgrade databases as required to maintain conformity with VA enterprise versioning standards;
- Provide database administration for all tools supporting development and testing to include load generator software;
- Provide Database Maintenance Log.

Deliverables:

- D. Bug and Error Report
- E. Database Maintenance Log

5.5.8 DATABASE MIGRATION SUPPORT

- The Contractor shall provide database migration support for all the VA-BIT applications it supports that are hosted in the VEMS Hosting cloud. This is an ongoing activity that the Contractor is required to support as emerging programs are identified to be transitioned to VEMS.
-

As part of database migration support, the Contractor shall:

- Migrate an existing database schema to an updated database schema as required (i.e., migrate data from a legacy database to a modified database);

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Support modification of the database schema as required.

5.5.9 OPERATIONAL SUPPORT

The Contractor shall support routine operations from 6:00 AM to 10:00 PM EST, Monday through Friday except for federal holidays for applications specified as standard operations for the Non-Core application. The Contractor shall provide 24x7 support 365-days per year for the VA-BIT applications specified. The Contractor shall support applications in the FISMA moderate and/or FISMA High environment and/or shall ensure the use of FedRAMP-defined controls and processes in accordance with VA's current FISMA ratings. The Contractor shall also be required to provide on-call 24/7 operations 365 days per year to support emergency maintenance requirements for the applications, which are 6AM to 10 PM EST and are categorized as Severity 1 production incidents. The Contractor shall:

- Use the following toolsets for operations and maintenance support:
 - VA Provided GFE;
 - NSD SDM – VA will provide access to SDM;
 - MS SharePoint (VA tool that the Contractor will be given access to) and the MS Office product suite (can be accessed through CAG or Contractor can provide);
 - RTC - VA will provide licenses;
- Coordinate with VA and other support Contractor personnel to manage and document operational support ticket routing and workflow.
- Evaluate, research, and respond to production support issues, which include application-specific trouble tickets and reports of defects;
- Receive, evaluate, research, and respond to trouble tickets in the Issue Tracking Tool. Unless directed otherwise by the COR, the Contractor shall address all application-specific trouble tickets in the following hierarchical order: by priority, date the ticket was created, urgency, and impact;
- Document and track production support issues that are considered application defects as Defect Work Items in the appropriate toolset and map them to the existing requirements for defect resolution. All defects shall be recorded and updated in the Rational Tool Suite;
- Develop Root Cause Analyses Reports for Priority 1 trouble tickets and Severity 1 defects;
- Develop After Action Report (AAR) for all Priority 1 and 2 and Severity 1 and 2 production support issues;
- Identify, develop and deploy bug fixes to defects by severity level, priority, and the date the defect was reported, unless directed otherwise by the COR. For each sustainment bug fix/hot fix release to Production, the Contractor shall provide a Sustainment Bug Fix/Hot Fix Release Package in Rational Tools, consisting of the following artifacts as currently required by the VA Release Readiness Office:
 - Upload the following into Change and Configuration Management (CCM)
 - > Source Control > Documentation Stream in Rational:

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- 1) Version Description Document (VDD)
- 2) Defect Log
- 3) Updated Installation/Back-Out/Rollback Plan
- 4) If defect repair is addressing a 508 compliance issue, also upload the Section 508 compliance verification test results and any additional 508 compliance documentation required by the VA Section 508 Office.
- 5) If a defect repair will change/impact any security features or controls, the Contractor shall perform a Fortify Scan of the software and upload the scan results (the results shall also be provided to the Security Team in order to update A&A documentation as required to maintain the hosting and application ATOs).
- b. Meet the Severity Level task requirements as outlined in the table below.
- c. Provide Incident, Problem, Event Management Reports with the following metrics:
 - 1) Defect Backlog - Quantity closed, reassigned, revised, and those remaining open from the defect backlog assumed at completion of the phase-in transition
 - 2) Ticket Volume - Quantity received, closed, reassigned, new tickets created (by the Contractor), or those introduced due to new releases and as classified by severity. These metrics shall be referenced both as a weekly (or more frequently as directed) variable and a cumulative, running total throughout the contract period.
 - 3) Timeliness of trouble ticket resolution in accordance with the severity levels metrics below - to include average (mean and median) number of days to close a ticket, and average (mean and median) age of tickets. The source data used as the basis for these counts to include identification of date opened and date closed for each ticket will be made available upon the COR's request.
- Execute a minimum of two (2) sustainment bug fix/hot fix releases per application per year (12 months) in addition to the resolution requirements in the Severity Levels table below.

Deliverables:

- F. Root Cause Analysis Report
- G. After Action Report
- H. Incident, Problem, Event Management Report
- I. Sustainment Bug Fix/Hot Fix Release Package in Rational
- J. Report of RTC Defects, National Service Desk (NSD) Tickets and Cloud tickets per application

Severity Levels (Production Defects)

VA Business Intelligence (VA-BIT)TAC Number: **TAC-18-XXXXX**

Level	Definition	Requirement
Severity 1 – Critical – Inoperable	Defect prevents or precludes the performance of an operational or mission essential capability, jeopardizes security, causes the system, application, process or function to not respond or end abnormally. A work around does not exist or is not feasible. For example, call center staff is not able to use the tool to communicate with clinical staff, and/or each other regarding patient care, including telephone triage of patient symptoms, defects in firewall allow security breach or system event causes essential or end-to-end application failure.	Notification to VA: 1. Respond within 1 hour of discovery during business hours (6:00 AM to 10:00 PM EST) 2. Analyze and correct the issue, documenting Root Cause Analysis (RCA) and updating the RCA report daily until remediation is complete. 3. Alert the PM, COR, and VA OIT organizations with sustainment responsibilities to issues that are unrelated to the application code or architecture within 1 hour of discovery. 4. Review Priority 1 and Severity 1 issues that are unrelated to the application code or architecture with the PM and/or COR within 1 business day of discovery. 5. Generate, store, track and maintain an After Action Report (AAR) within 3 business days following remediation. AARs shall detail methods employed to resolve defects and efforts employed to minimize recurrence. 6. Contractor may be required to work extended hours as

VA Business Intelligence (VA-BIT)

TAC Number: TAC-18-XXXXX

		<p>severity 1 issues are worked until resolution</p> <p>Resolution: The Contractor shall resolve as soon as possible, with a team of resources working 24/7 until resolution. Resolution will result in an emergency release.</p>
Severity 2 – Major – Operable in degraded mode	<p>A process does not work as specified and/or produces an error that degrades or impacts the system or user functionality. A work around does not exist or is not feasible.</p>	<p>Notification to VA:</p> <ol style="list-style-type: none">1. Respond within 4 business hours of discovery. Business hours are 6:00 AM to 10:00 PM EST.2. Alert the PM, COR, and VA OIT organizations with sustainment responsibilities to issues that are unrelated to the application code or architecture within 1 business day of discovery. Generate, store, track, and maintain an AAR within 5 business days. AARs shall detail methods employed to resolve defects and efforts employed to minimize recurrence. <p>Resolution: The Contractor shall resolve as soon as possible but no longer than 3 business days, with a team of resources working 24/7 until resolution. Resolution may or may</p>

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

		not result in an emergency release.
Severity 3 – Average – Work around exists	<p>A process does not work as specified and/or produces an error that degrades or impacts the system or user functionality. A work around has been developed that provides the required functionality until a fix can be applied. A fix should be applied in accordance with the resolution timeframe. Examples are: valid data is not accepted, data recorded to the database is incorrect or incomplete, incorrect or incomplete data is displayed on-screen or in a report, an edit is missing against invalid data, or invalid edits occur against valid data.</p> <p>Other Considerations: Workaround requires significant field operations effort. System performance is degraded</p>	<p>Notification to VA: 1. Respond within 3 business days of discovery. 2. Alert the PM, COR, and VA OIT organizations with sustainment responsibilities to issues that are unrelated to the application code or architecture within 3 business days of discovery.</p> <p>Resolution: Any existing Severity 3 defects shall be addressed within 6 months or less of task order award. Hereafter, any new Severity 3 defects shall be resolved and included in a bug fix/hotfix release on a quarterly basis.</p>
Severity 4 – Minor	<p>Minor defect that is cosmetic or inconvenient but does not prevent user from using the system to accomplish their task. For example, the screen display or hardcopy report contains errors in</p>	<p>Notification to VA: 1. Respond within 3 business days of discovery. 2. Alert the PM, COR, and VA OIT organizations with sustainment responsibilities to issues that are</p>

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

	<p>spelling, grammar, or alignment, navigation is inconsistent, or error messages are incorrect. Minor defect fixes can be applied as schedule allows.</p> <p>Other Considerations: Defect affects few field employees Defect has little or no potential for adverse publicity</p>	<p>unrelated to the application code or architecture within 3 business days of discovery.</p> <p>Resolution: Any existing Severity 4 defects shall be addressed within 6 months or less of task order award. Hereafter, any new Severity 4 defects shall be resolved and included in a bug fix/hotfix release on a quarterly basis.</p>
Production Support Issues	<p>For all production support issues, regardless of priority or severity, the Contractor shall:</p> <ol style="list-style-type: none">1. Update trouble tickets with the current status and a description of the solution or activities in progress to resolve the trouble ticket.2. Document and track production support issues that are considered application defects as Defect Work Items in RTC and map them to the existing requirements for defect resolution.3. Request approval from the COR to change the priority and/or severity of a production support issue when the Contractor believes the	<p>Notification to VA: Status updates shall be completed each time the status of a ticket changes within 24 hours of the change.</p>

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

	priority and/or severity level is incorrect.	
--	--	--

Priority Levels (Lower/Non-Production environment defects)

PRIORITY	DEFINITION
Priority 1 - Resolve Immediately	Further development and/or testing cannot occur until the defect has been repaired. The system cannot be used until the repair has been affected.
Priority 2 - Give High Attention	The defect must be resolved as soon as possible because it is impairing development and/or testing activities. System use will be severely affected until the defect is fixed.
Priority 3 - Normal Queue	The defect shall be resolved in the normal course of development activities. It can wait until a new build/version.
Priority 4 - Low Priority	The defect is an irritant that shall be repaired but only after more serious defects are fixed.

5.5.10 TESTING SUPPORT

- The Contractor shall provide maintenance testing support services as part of the support for VA-BIT. The VA-BIT maintenance testing services shall include all end-to-end testing. The Contractor shall ensure completion of all the tasks and deliverables detailed in Section 5.2.2.6 (Testing) for each release.

5.5.11 TECHNICAL SUPPORT

The Contractor shall:

- Participate, facilitate, and document design proposal impact due to maintenance work and attend change management meetings;
- Analyze the outputs of the change management process;
- Provide design proposal update recommendations for optimization, proactively as adaptive and preventive sustainment, as well as reactively for corrective sustainment and to address trouble tickets. The Contractor shall provide meeting agendas and minutes from the design requirements meeting(s);
- Facilitate technical meeting(s) with VA business users and technical staff supplying analysis in regards to defect management/code enhancements to

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

identify how the user requirements will continue to be met and to determine technical reusability, modification of service components, and continuity of integration with VA systems interfaces.

- Conduct a design concept review meeting to formally present the design to VA technical staff and the business sponsor(s) to ensure the design meets the intent of sustainment requirements. The Contractor shall provide meeting agendas and minutes from the design concept review meeting(s);
- Maintain and update the existing Architecture Design Document to ensure integration with the VA system interfaces;
- Maintain and update the existing Data Schemas that map data to each VA system interface. The Contractor shall facilitate coordination with the projects that support the systems with which VA-BIT interfaces.

5.5.12 TECH REFRESH

The Contractor shall ensure all features, functionality, and capabilities that were present in production will remain. This includes user interface look and feel, workflow, automation, and interfaces with other applications. In support of these tech refreshes, the Contractor shall apply the same life cycle tasks described in section 5.2.

5.5.13 COTS SOFTWARE PATCHES

The Contractor shall support the Cloud Hosting Team as needed in order to deploy COTS software patches (as required/recommended by the vendor of the COTS Software for security or 508 conformance fixes. These software patches are anticipated to occur 10-20 times per month.

5.5.14 SERVICE DESK SUPPORT

The Service Desk is a component of the overall Production Incident Escalation Communication process. All user support calls are initially sent to the VA NSD, which is responsible for Tier 1 support within the Production Incident Escalation Communication process. VA NSD uses the Service Desk Manager (SDM) tool to track all support calls. VA NSD will address any issues with the desktop, user access, network access, and printing.

Any issues that are specifically related to the VA-BIT Applications shall be forwarded to the Contractor Service Desk, which is responsible for Tier 2 support within the Production Incident Escalation Communication process for resolution.

The Contractor shall:

- Operate the Service Desk to provide all required Tier 2 support.
- Respond to all issues that the VA NSD identifies as Tier 3 or Tier 4 VA-BIT issues. Tier 3 and Tier 4 support

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Support the Service Desk from 6:00 AM to 10:00 PM EST, Monday through Friday except for federal holidays for Non-Core applications. Support 24x7/365 for applications specified as VA-BIT applications;
- Provide on-call personnel to support resolution of critical and serious severity code tickets for Tier 2, 3, or 4 issues received from the VA NSD after hours.

Incident Reporting and Notification Process Flow

VA NSD Production System SLAs

Code	Customer Impact	Response to Customer	Resolution Goal
1 – Critical	Production System Unavailable	0-15 minutes	0-2 business hours
2 – Major	Production System Delayed (Potential Impact on Business Function)	0-60 minutes	2-4 business hours
3 – Average	Production and Preproduction (Available - No Business Impact)	0-4 business hours	4-8 business hours
4 – Minor	New Service/Program Addition		

5.5.14.1 TIER 2 SUPPORT

The Contractor shall provide Tier 2 support to include the following:

- Review the issue information provided through the NSD and respond to the customer in accordance with the SLA defined in the above table;
- Use the SDM tool, provided through the VA NSD, to retrieve Tier 1 ticket information in support of Tier 2 resolution;
- Contact the customer/user if more information is required, to provide resolution recommendations, or to provide a status. All information gathered shall be provided to the Service Center to update the Remedy ticket;
- Contact the customer/user and provide a recommended resolution to the issue, including a workaround provided by the business sponsor, where available. The Contractor shall walk the user through the resolution recommendation. The Contractor shall document resolution results and provide the information to the Service operator for entry into the SDM ticket. The Contractor shall update the SDM ticket with the resolution so that the Tier 1 service providers can use to assist users experiencing the same issue;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Contact the customer/user and provide one-on-one training support to walk the user through the operation of the system if the issue is the result of a known user error. The Contractor shall document the training provided to the Service operator for entry into the SDM ticket;
- Gather enough additional information, including at a minimum, verbal details, emailed Incident Report forms, and screenshots to determine the severity of the incident; the severity level in accordance with the SLA table shall be logged in the SDM ticket;
- Notify the Government VA Service Desk Manager and present all the information about any incidents that are determined to be a severity code 1 or 2;
- Support crisis incident escalation processes, including transferring the incident to the Triage 1 Team, and contacting VA-BIT Project Management. If the incident is determined to be a severity code 3, the Contractor shall attempt to replicate or troubleshoot the incident as part of the incident verification/validation process. If the severity code 3 issue cannot be resolved, the Contractor shall transfer the Incident to the Triage 1 Team and contact VA-BIT Project Management. For all issues forwarded to the Triage 1 Team, the Contractor shall continue to interface with the customer/user to request more information and to update status. After the customer/user is notified of the resolution or incident transfer and is satisfied with the actions taken, the Contractor shall ensure that the resolution fixed the issue and shall update and close the incident ticket;
- Support application end user account provisioning in the Production and subordinate environments. This includes creating, retrieving/resetting, updating, and deleting accounts.

The Contractor providing Tier 2 Support is the only level to have initial or follow up contact with the customer for customer management support.

5.5.14.2 TIER 3 AND 4 SUPPORT

The Contractor shall:

- Submit all issues that cannot be resolved by direct interface to the customer/user for Tier 3 Support to the Tier 3 Site Operation Teams using the SDM system, program log, and during daily communication. The Contractor shall ensure that the VA-BIT Program Manager and COR is aware of the severity code and the time when the incident was reported;
- Support the Triage 1 Team in coordination with the Tier 3 Site Operation Teams. Operations Support Team members are as follows: Lead Engineer; Operations Support Team; Information Assurance Team; and the Maintenance team. The Triage 1 Team shall assess the scope and impact of the unresolved incident, and determine if the incident relates to problems associated with:
 - Infrastructure
 - Application/Development
 - Other interfaces as defined in section 5.2.3.
 - User Error

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- Access Control
- Slow Performance
- Lost Data
- Incorrect Data
- Requirement Request
- System Outage

Deliverables:

- K. Service Desk Response Scripts
- L. Statistical / Analytical Reports

5.5.14.3 SERVICE DESK DOCUMENTATION AND REPORTING

The Contractor shall:

- Report all Service Desk issues identified as critical issues to the COR within thirty (30) minutes of receipt. Reports of actions being taken to resolve the issue shall be provided with updates hourly until full functionality is restored. A Detailed Outage Report that documents the outage time, services impacted, cause of the outage, and actions taken to restore the system shall be produced by the Contractor after the incident is resolved and provided to the COR;
- Provide a Service Desk Monthly Progress Report which documents issue status and Service desk metrics for all issues identified within a given month. The Contractor shall maintain an issues log with the issues reported, severity of the issue, response time, and resolution. The issues log shall be delivered with the Service Desk Monthly Progress Reports. The issues log shall include the date and time when the issue was reported, the person reporting the issue, the location reporting the issue, the severity code, the cause of the issue, a description of the issue, a workaround for the issue if relevant, the date and time the workaround was provided, the final solution to resolve the issue, and the resolution date and time. The cause categories shall include, at a minimum, system outage, user error, slow performance, lost data, incorrect data, and access control. The issues log for a specific time period shall be provided to the COR upon request;
- Maintain service desk and reporting metrics, which shall be documented within the Service Desk Monthly Progress Reports. The following metrics shall be included:
 - The number of issues by severity code
 - The number of issues by location
 - The number of issues by Cause
 - The number of user error issues by location
- Support weekly Executive Board and weekly "Pulse Check" meetings hosted by Senior OI&T, and Senior VBA/VHA leadership and provide status updates for high priority urgent issues. The Contractor shall respond to all requests for information regarding service desk, problem tickets;

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

Deliverables:

- M. Detailed Outage Reports
- N. Service Desk Monthly Progress Reports

5.6 PHASE-OUT TRANSITION SUPPORT

The Contractor shall:

- Develop and deliver a Phase-Out Transition Plan in the event that all or part of the tasks are terminated or completely transitioned to the Government or a new Contractor at the end of the period of performance. The Contractor shall submit details for the Phase-Out portion of the Transition Plan, and execute the Phase-Out Transition Plan upon Government approval. The Transition Plan may be exercised by the Government anytime during the base and/or option periods. All transition actions shall be completed prior to end of PoP. The Contractor shall provide SME support for 30 days to affect the requisite knowledge transfer in accordance with the resulting Transition Plan and schedule. At a minimum, the Transition Plan shall include the following:
 - o Roster of key POCs with email address and telephone numbers
 - o Transition timeline with key milestones
 - o Data/databases
 - o Inventory and transition of historical data (e.g., memos, letters, correspondence, regulations, reports, documents, transition agreement documents, software licensing agreements, hardware maintenance agreement, memorandums of agreement/ understanding, and inter-service agreements)
 - o Procedural manuals/guidelines
 - o Operating instructions
 - o Data and workflow process
 - o Application scheduling process
 - o Templates used in day-to-day operations
 - o Orientation to introduce incumbent Contractor team, programs, and users to the incoming team, explaining tools, methodologies and business processes
 - o Procedures to introduce Government personnel, programs and users to the Contractor team's tools, methodologies and business processes
 - o Strategy and approach regarding personnel staffing and training during the transition period
 - o Process for transfer of on-hand inventory, if applicable
 - o Transition checklist
 - o Signed turnover agreements
- Work collaboratively with other support Contractors and/or Government personnel. As part of collaboration, the Contractor shall convey any and all information, as it pertains to VA-BIT projects, its processes, diagrams and any reports that emanates from the system that may be requested to support this collaboration. This support shall also consist of providing advice, clarification or explanation to facilitate the understanding of the information presented.

VA Business Intelligence (VA-BIT)

TAC Number: TAC-18-XXXXX

Deliverable:

A. Phase-out Transition Plan

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/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63, VA Handbook 6500 Appendix F, "VA System Security Controls", and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of Personal Identity Verification (PIV) and/or Common Access Card (CAC), as determined by the business need. Assertion based authentication must include a SAML implementation. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST 800-63 guidelines. Trust based authentication must include authentication/account binding based on trusted HTTP headers. The Contractor solution shall conform to the specific Identity and Access Management PIV requirements set forth in OMB Memoranda M-04-04, M-05-24, M-11-11, as well as the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. 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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf> respectively. The identity authentication Level of Assurance (LOA) requirement for this specific effort is LOA-4.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005

(<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267 (<http://www-x.antd.nist.gov/usgv6/index.html>), the Technical Infrastructure for USGv6 Adoption (<http://www.nist.gov/itl/antd/usgv6.cfm>), and the NIST SP 800 series applicable compliance (<http://csrc.nist.gov/publications/PubsSPs.html>) shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack IPv6 IPv4 connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack IPv6 IPv4 users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack IPv6 IPv4 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf>), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 2013 and Windows 8.1. However, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Office 2013 and Windows 8.1 individually as the VA standard, Office 2013 and Windows 8.1 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 Contractor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) specific to the particular client operating system being used.

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

The Contractor shall utilize ProPath (PAL), the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

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

- 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 (Refer to Section 4.6 of the Task Order PWS for investigative requirements by task), etc. The Contractor

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within one day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.

- 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:
 - 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 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. If the background investigation determination is not completed prior to the start date of work identified in each Task Order, a Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.
- k. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the TO.
- l. 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.
- m. 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.
- n. 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.

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.5	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.6	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

- a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
- b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and SubContractor employees to the COR to begin their background investigations in accordance with the ProPath (PAL) 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 to. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
- d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after to award:
 - 3) Optional Form 306
 - 4) Self-Certification of Continuous Service
 - 5) VA Form 0710
 - 6) Completed SIC Fingerprint Request Form
- e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/to. 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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	<ol style="list-style-type: none">1. Demonstrates understanding of requirements2. Efficient and effective in meeting requirements3. Meets technical needs and mission requirements4. Provides quality services/products	Satisfactory or higher
B. Project Milestones and Schedule	<ol style="list-style-type: none">1. Established milestones and project dates are met2. Products completed, reviewed, delivered in accordance with the established schedule3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Project Staffing	<ol style="list-style-type: none">1. Currency of expertise and staffing levels appropriate2. 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 the Government2. Services/products delivered were of desired quality	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.5 FACILITY/RESOURCE PROVISIONS

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

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath (PAL), Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 to consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

The Government shall provide access to VA's approved configuration management tool, which is currently IBM Rational Collaborative Application Lifecycle Management (CALM) Toolset (hereafter referred to as Rational) after contractor personnel complete the six web based training modules as specified in Section 5.1.6 and obtain VA network access. The Rational toolset is used by VA to provide a single Agile product application lifecycle management tool to track project execution details. The Contractor shall work with its respective point of contact, to obtain access to TMS to take the mandatory training courses.

The VA COR will provide the following Government Furnished Materials/Information/Equipment upon to award and as soon as all security and privacy training is complete, background investigations have been initiated in the e-qip system and network access has been granted for performance of this to:

- a) VIP data and documentation
- b) Access to VA Project Management Tools and Repositories including:
 - i. ProPath
 - ii. Rational Tools access after Rational training is completed
 - iii. Primavera/Microsoft Project scheduling tools as mandated at the time of the PoP
- c) VA Account and Network Access (Virtual Private Network (VPN), if Government Furnished laptops are provided or Citrix Access Gateway (CAG) access if the Contractor's laptop is to be used to conduct work associated with this requirement,
- d) VA email account
- e) VA PIV card received

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific requirement. The Government also understands that GFE is limited to Contractors requiring direct access to the network to: access development environments; install, configure and run TRM-approved software and tools (e.g., Oracle, Fortify, Eclipse, SoapUI, WebLogic, LoadRunner, etc.); upload/download/ manipulate

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

code, run scripts, apply patches, etc.; configure and change system settings; check logs, troubleshoot/debug, and test/QA.

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

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 to 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 to incorporates VA Handbook 6500.6, "To Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "To Security" shall also be included in every related agreement, to 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.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 to 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 to, 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 to deliverables for EA compliance prior to acceptance.

VA Internet and Intranet Standards

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

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

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

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

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

Section 508 – Electronic and Information Technology (EIT) Standards

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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:

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

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.

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.

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 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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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

Deliverables:

- A. 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 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 to.

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.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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 to. The Contractor shall release no information. Any request for information relating to this to 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 to. 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 To and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for to 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 to, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this to 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 to, 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.

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

- d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
 - e. VA, as well as any Contractor (or SubContractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
 - f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
 - g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
 - h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this to, 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 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

VA Business Intelligence (VA-BIT)

TAC Number: **TAC-18-XXXXX**

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. The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products”.
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.