# PERFORMANCE WORK STATEMENT (PWS)
# DEPARTMENT OF VETERANS AFFAIRS

**Office of Information & Technology**
**Product Engineering Service (PES)**

**Data and Analytics Integrated Modernization and Operations (DAIMO)**
**Data-centric Systems Development, Modernization and Sustainment**

**Date: 11/22/2023**
**VA-24-00013843**
**Task Order PWS Version Number: 0.3**

# Contents

# 1.0 BACKGROUND

The Department of Veterans Affairs (VA), Office of Information & Technology (OI&T), Product Engineering Service (PES), Data and Analytics Pillar (DA) maintains a vision to provide positive outcomes for Veterans and their families through the enablement of a data-driven VA culture that continuously improves the delivery of world-class benefits and services. This vision is supported by PES DA’s mission to deliver an integrated ecosystem of interoperable data management, discovery and analytics tools that enable evidence-based decision making grounded in the adoption of authoritative data sources across the VA Enterprise. PES DA manages a complex portfolio of platforms and products that empower the VA and OI&T specifically to support the increasing demand for data to meet the Department’s obligations to the Veteran community. PES DA is charged with ensuring VA’s enterprise data assets are artificial intelligence (AI) ready.

OI&T modernization and t Sergeant First Class (SFC) Heath Robinson Honoring our Promise to Address Comprehensive Toxics (PACT) Act initiatives are accelerating demand for advanced AI-based solutions and VA’s core data management capabilities are critical to the achievement of the Department’s goals, and PES DA must continue to evolve the Summit Data Platform (SDP) to support the modernization of the enterprise data management lifecycle. This will ensure the tools, best practices and supporting architecture continually evolve to meet the needs and expectations of OI&T’s technical product teams. Furthermore, evolving the platform and maintaining high availability of essential products and services is increasingly important to PES DA’s objectives to achieving the VA’s mission.

## 1.1 Data and Analytics Integrated Modernization and Operations (DAIMO)

Data and Analytics Integrated Modernization and Operations (DAIMO) will consolidate the development, enhancement, and modernization and daily operational sustainment of products and programs executed by the DA of the PES. PES DA also manages the Data and Analytics Product Line (DAPL) for VA OI&T and facilitates efforts across VA and with external partners to foster the secure, timely and accurate sharing of trusted data products that enable the delivery of healthcare and benefits to the Veteran community. Data-centric products managed in the DAPL are in various stages of their modernization journeys. In some cases, this calls for the consolidation of capabilities from multiple products to be delivered on robust, developer friendly platforms that enable rapid integration by technical teams across the Department. In other areas, the need to reevaluate the approach, design and engineer utilizing modern patterns is necessary to realize a scalable architecture capable of meeting the needs of a digital first VA.

PES DA strives to provide thought leadership to innovate and drive the adoption of leading-edge technologies to positively impact Veteran outcomes, enable a highly resilient availability posture, standardize and improve all aspects of the DevOps processes and practices supporting its products and platforms. This includes, but is not limited to, capabilities for proactive monitoring including synthetic transactions where appropriate, optimizing infrastructure as code, and unifying the continuous integration/continuously delivery (CI/CD) product development and deployment practices across PES DA portfolio. PES DA is responsible for platform and product health monitoring described above, and communicating root cause of detected defects, performance issues and other production disruptions that may impact the consistent availability, performance and integrity of Pillar ecosystem. DAIMO will address the ongoing sustainment needs of the programs and products discussed in the following sections.

As VA continues the adoption of a product mindset for information technology solutions, PES DA will progressively evolve each Pillar’s offerings in concert with our business partners. PES DA will continue to define modernization goals for each product and platform to ensure that capabilities delivered to VA reflect the evolving state of the industry.

PES DA has identified two overarching target state platforms that will enable the consolidation of product capabilities across the Pillar. SDP is the target modernization state for legacy data management, reporting and analytics development products and programs within the DA Pillar. SDP will enable the future development of enterprise Machine Learning (ML) and Artificial Intelligence (AI) solutions and will provide self-service capabilities to technical teams across OI&T to build and serve source and domain aligned data products. VA Profile will deliver the enterprise’s Master Data Management (MDM) capability and will enable the transactional delivery of key master data products to IT products and systems across the Department.

The intended target state of the Pillar’s ecosystem to minimize duplication of technology stacks and drive commonality in required skills will permit service providers to focus on a reduced footprint of skillsets once the target state architecture is realized.

## 1.2 VA PROFILE

VA Profile is the authoritative data source for VA customer contact information and the authoritative service for VA common data. VA Profile provides VA customers the ability to update information and have a 360° view of their Master Record. This improves data quality and management of the Veteran Profile through implementing business rules and exception handling within the solution, as well as enterprise data governance (policy, procedures, etc.). The customer record is readily available for the Veteran and VA staff to view.

VA Profile modernizes VA systems by ensuring that customer common data is synchronized and shared across the VA, regardless of the channel used to update the information. Synchronizing data across the three major Veterans Benefits Administration

(VBA), Veterans Health Administration (VHA), and National Cemetery Administration (NCA) systems is just one step in synchronizing all VA systems. Currently, VA Profile is integrating with new VA systems and business lines so Veterans' identity, contact information, military service, enrollment, eligibility for VA services and benefits, socio-economic, demographic, customer experience, interaction history and shared data from VHA, VBA, and NCA are automatically synchronized across all VA systems.

VA Profile employs an enterprise MDM solution that provides a capability to supply a cleansed, singular, authoritative set of information encompassing all applicable data subject areas shared among multiple Lines of Business (LoBs). MDM data updates are propagated to relevant consuming systems in all applicable LoBs; VA customers will be enabled to update contact, demographic and socio-economic information for immediate propagation VA-wide to avoid the need for duplicate data entry.

In the VA Enterprise Cloud (VAEC), VA Profile utilizes a service platform that hosts distinct software microservices to encapsulate specific functional needs. Data subject area payloads are transmitted and received in business provided subject models, referred to as Business Information Objects (BIOs). Within the accreditation boundary of VA Profile to support scale, message volume tuning, and system resilience within the service mesh, asynchronous messaging is leveraged. LoB or Enterprise Systems integrate with VA Profile as either a Direct Consumer Integration, or as a Synchronization Partner.

Direct Consumer Integration – VA Profile direct consumer integration communicates with the Common Update Framework (CUF) Data Hub via industry standard REpresentational State Transfer (REST) Application Programming Interface (APIs) using commodity tools. The Hub provides RESTful microservices to push and pull data from the Longitudinal Veteran Record by issuing HTTP requests that transmit and receive a BIO. The single set of APIs is technology agnostic enabling consumer applications to interact with VA Profile in both attended and unattended flows.

Synchronization Partner – In collaboration with a LoB system owner, VA Profile implements a Change Data Capture (CDC) or Web Service / API based method to capture all operations taken.

## 1.3 VETERANS INFORMATION ELIGIBILITY REPORTING SYSTEM (VIERS)

Veteran Identity/Eligibility Reporting System (VIERS) is a system providing middleware services that support access to consuming applications such as:

- Affordable Care Act (ACA)
- Airborne Hazards Burn Pit Registry (AHOBP)
- Digits-to-Digits (D2D) Veterans Service Organization (VSO) Claims Processing
- Outreach Reporting Tool
- eBenefits

- Veteran Online Health Application (VOA)
- Veterans OnLine Application (VONAPP) Direct Connect (VDC)
- Stakeholder Enterprise Portal (SEP)
- Customer Relationship Management (CRM)
- Voice Access Modernization (VAM)
- Enrollment System (ES)
- Veteran Benefits Management System (VBMS) and Chapter 33 (CH33)
- Federal Case Management Tool (FCMT)

VIERS services function as a middleware (based on WebLogic and WebSphere) using a Service Oriented Architecture (SOA) providing services for: submitting electronic forms, validating Master Veteran Index (MVI), correspondence, event notification, claims submission (Benefits Gateway Services (BGS)/CGS) and various data stores established in the data layer such as Corporate, Beneficiary Information Record Locator System (BIRLS), Administrative Data Repository (ADR), and Master Veteran Index (MVI).

The VIERS suite of middleware services provide orchestration to Military Service Data Sharing (MSDS), Digits-to-Digits (D2D), Claims Processing & Eligibility (CP&E) Adapters, CP&E Eligibility service, CP&E Beneficiary service, Business Event Notification Service (BENS), Affordable Care Act (ACA) Enrollment Verification Service, Veteran Person Adaptor Service, Veterans Appeals Control and Locator System (VACOLS) adapter, reporting and analysis warehouse, .

## 1.4 VA DOD IDENTITY REPOSITORY (VADIR) AND VETERANS INFORMATION SOLUTION (VIS)

VA Department of Defense (DoD) Identity Repository (VADIR), Veterans Information Solution (VIS) provides a database and Graphical User Interface (GUI) to store data and web services to consuming applications, such as, Enrollment Systems, Veterans Access, Choice, and Accountability Act (VACAA), aka Veterans Choice (VC), Patient Protection/Affordable Care Act (ACA), ChampVA, Veterans Online Application (VONAPP), Business Events Notification Service (BENS), Identity Management System (IAM IdS), etc. VADIR and VIS are hosted in the AWS Cloud.

VADIR functions as a database and middleware using a SOA approach to provide orchestration according to business rules, with services that crosscut among various business capabilities including electronic forms, storing images and validation of MVI. VADIR is a service/program provider for Veterans Information Solution (VIS) which display a GUI for VADIR data.

The VADIR database serves as the authoritative data store from the DoD and VA sources for all military service records (for those currently serving, transitioning, and/or separated members and veterans)  to support eligibility decisions to include registration, automated eligibility determinations, common business functions, and consistent identification of beneficiaries across VA, providing the data to support the improved veteran-centric services that support enterprise goals and the determination of legislatively mandated Veterans' benefits. VADIR provides reporting and analysis capability to VA staff offices and LoBs. VADIR provides real-time notification of critical events across to service member care and benefits which can be applied across VA as needed. VADIR database is built in an Oracle – Red Hat Linux operating system. VADIR Web Services are on the RedHat Linux operating system and use the Apache web server and WebLogic application server.

VIS is a web-based query application that provides a consolidated GUI view of VADIR data for the VBA and the DoD. VIS enables authorized users to search records and retrieve information on the Veteran's or Service member's profile or military history; on certain education benefits; and information on compensation and disability pension ratings and awards and on dependents included in those awards. VIS is a SOA -based application that leverages the Java Enterprise Edition (Java EE) technology stack. The application is packaged in Web Archives (WAR) and deployed to WebLogic on a clustered group of managed servers that are load balanced via the Apache web server and its WebLogic plugin. The web server and application server run on Red Hat Enterprise Linux.

## 1.5 HEALTH DATA REPOSITORY (HDR)

Health Data Repository (HDR)/Clinical Data Service (CDS) is a national repository of clinical information which stores discrete data. CDS is the data abstraction layer that applications utilize to retrieve and send data to the HDR. On one national platform and provides a national, longitudinal data base of veteran's clinical data that is structured, standardized and used by clinical & analytic applications.
Below are details of the HDR product/service:

HDR serves as the authoritative data store for nationalized clinical programs such as Home Telehealth and MyHealthVet and other non-VistA clinical applications. Healthcare providers use the HDR and VistA to facilitate longitudinal patient-centric care, storing patient-centric clinical data in a computable format that can be used by other applications for analytical purposes. The HDR database is developed in Oracle and the Clinical Data Service (CDS) and Pathways access layer in Structured Query Language (SQL), Java, and PL/SQL with interfaces to WebLogic. WebLogic is responsible to interface with the access layer.

## 1.6 CORPORATE DATA WAREHOUSE (CDW)

Corporate Data Warehouse (CDW) provides national authoritative health and enterprise data and analytic tools at scale to 23,000+ developer/analysts from 7,500+ workgroups. These workgroups create downstream data products that get consumed by 100,000+ content customers including Veterans, Congress, Inter-agency partners, VA Senior

Leaders, Health Research, and National/Field Healthcare Operations. CDW provides the authoritative health data for the VA. It also integrates other Enterprise Financial and Administrative data sources. These resources are critical to maintain CDW which is a large complex critical data ecosystem with thousands of downstream dependencies.

Core services include development and implementation of Structured Query Language (SQL) Server Integration Services (SSIS) Enterprise Architecture, SQL Server Analysis Services (SSAS) Enterprise Architecture, Pyramid Analytics Enterprise Architecture, and SharePoint Enterprise Architecture. Core services also include Extract-Transform-Load (ETL) programming using SSIS to support adding new data domains to the CDW, creation and maintenance of SQL Server Analysis Services (SSAS) cubes, CDW Enclave Windows System Administration services, Cache Shadow support services, and CDW Customer Service support.

## 1.7 SUMMIT DATA PLATFORM (SDP)

The SDP is VA's cloud-based Enterprise Data Analytics platform serving VA's Administrations and Staff Offices. The SDP enables governed access to VA data integrated with a comprehensive analytics toolset for data analysis and research teams to derive valuable insights, uncover patterns, and make data-driven decisions to benefit veterans. The SDP enables self-service analytics: IT/Analytics teams from across the VA can fully leverage the platform for their needs with minimal interference. The SDP also offers "White Glove" services to VA lines of business who have mission critical needs but might lack analytical skillsets.

## 1.8 CUSTOMER EXPERIENCE DATA WAREHOUSE (CXDW)

The Customer Experience Data Warehouse (CxDW) uses advanced data intake, conditioning, and curating techniques to provide business-actionable customer experience data analyses to diverse VA Customers and external entities with similar data management needs. Further, CxDW extends their data management services to other VA entities with data management needs and provides them with business actionable data analyses for their customers.

CxDW enables The Veteran Experience Office (VEO) to gain insights into the full encompassing experience of VA customers. It converts conditioned and refactored data into a consistent, common data model that can be used across the enterprise. It is a cloud data service product that allows other data platform owners to offload reporting and analytics overhead while also supporting a centralized repository of VA data.

## 1.9 VETERANS INFORMATICS AND COMPUTING INFRASTRUCTURE (VINCI)

The Veterans Informatics and Computing Infrastructure (VINCI) mission is to provide high-quality data, openly extensible information technology, and supporting services to generate and integrate new knowledge, methods, and technologies for research and medical-care communities to assess and improve Veterans' healthcare. VINCI's vision is to be part of a vital private-public community in which open-source and open-standards technologies provide a foundation for generation of new content and technologies to promote transparent and reproducible health science and business intelligence. VINCI provides Cloud based computing for no charge in the VA to authorized individuals and groups. VINCI offers Statistical Analysis for System (SAS), MATLAB, STATA and a host of analytic analysis software. VINCI will help researchers develop patient cohorts specific to their operational or research needs.

VINCI Research Program's mantra is innovation and translation for dual research and operational medical-care benefit. Health Systems Research and Development (HSR&D) and VA in general, recognizes that for a sustainable, relevant, and vibrant program, the Program must serve a dual mission that supports health services research and innovative business intelligence. The following statements of mission, vision, and value are from the perspective of research. For a broader perspective, researchers could be interchanged with business-intelligence innovators and practitioners. VINCI Research Program's mission is to provide services to help researchers and clinicians appropriately access data and use tools, to conduct research addressing key gaps in VINCI's offerings, and to manage the interface with IT partners for translating research innovations into deployed tools for general use. VINCI Research Program's vision is an enticing, cooperative scientific infrastructure that provides a majority of HSR&D funded projects with transparent methods and reusable tools resulting in reproducible results.

VINCI utilizes the Corporate Data Warehouse (CDW) which is the central collection of standardized databases integrating key enterprise-wide clinical, administrative, and financial data to provide a unified view of VA data. In addition to CDW data, VINCI uses data from National Institute of Health (NIH), Center for Medicare and Medicaid Services (CMS), DoD and other data sources. The CDW strategy includes standard information, standard architectures, and standard tools that management needs to have access to data to support management decision making. The Business Intelligence Services Line (BISL) requires support services for the CDW teams. VINCI is a research and development partnership and clinical operational platform for health services research, epidemiology, decision support, and business intelligence; and its partners are the VHA HSR&D program, VHA's Office of Informatics and Analysis, and OI&T BISL. All participating groups desire that their contributions be managed as an integrated organization, the impact of which will be much greater than the sum of its parts.

Since VINCI has expertise in the Veterans Health Information System and Technology Architecture (VistA) Electronic Health Record (EHR) data, other VA projects will call upon this expertise to further the larger mission of OI&T to assist in data migrations, transformations and conversion to Cerner or other formats. Also, as VA Community Care progresses more data sources will become available and VINCI will need to be able to incorporate those sources in the support pool of data. These are potential data sources that will be valuable in the VINCI environment. In addition to the data support, a research Natural Language Processing (NLP) effort yielded some versatile software that will be used for search in both the commercial software and VistA environments. It is expected that enhancement and sustainment of this effort will be supported by VINCI.

VINCI brings together data sources and provides the analytical environment for performing studies, data stewards such as VHA National Data Systems (NDS), VA Information Resource Center (VIReC), Oak Ridge National Labs (ORNL) and others that authorize research access to patient data. This potentially could include Cerner, Community Care, and other initiatives in the future. New research projects are granted access to dynamic views or snapshots of data that can be updated as needed. In addition to data storage, VINCI includes a cluster of servers set aside for tasks like analysis, data processing, and extracting information from text. This means that VA researchers will have access to data and the applications they need to select, transform, and analyze patient data in a central, secure location accessible from the VA intranet.

## 1.10 ROBOTICS PROCESS AUTOMATION (RPA)

The VA Robotic Process Automation (RPA) Center of Excellence (COE) provides VA customers with services they need to start and maintain and successful RPA Program. These include security and privacy governance, purchasing of licenses; acquisition of integrator services; RPA program support; RPA system integrator network; and best practices. The VA RPA Platform provides Secure platform environment maintained by the VA within the VA Enterprise Cloud with a High Authority to Operate (ATO) with ongoing maintenance and support from the VA COE. Two leading RPA software solutions are available, UiPath and Blue Prism. Both solutions have Orchestration and runtime resources in Development, Pre-Production, and Production environments. Business rule-based AI/ML capabilities are available to automate use cases with AI needs.

## 1.11 OTHER PRODUCT ENGINEERING SERVICE DA (PES DA) PRODUCTS

The DAIMO system will continue to support a variety of PES DA products. These products may include applications created to access, examine and correlate data available in one or more of the platforms listed above. Such products include, but are not limited to:

- Access to Care (ATC)
- CDW-Electronic Quality Measurement (CDW-eQM)
- CDW Mental Health (MH)
- Coordinated Care Tracking System (CCTS)
- National Surveillance Tool (NST)
- VA Common Operating Platform (COP) (Palantir)
- PACT Act Data Mart
- Data Interoperability (DI)
- Federated Data Sharing with External Agencies

- Source and Domain Aligned Authoritative Data Products

## 1.12 DATA ACCESS SERVICE (DAS) ENTERPRISE SERVICE ENHANCEMENTS (DESE)

The Data Access Service (DAS) Enterprise Service Enhancements (DESE) project is the enhancement of DAS Core Phase 1 and 2 capabilities. Enhancements in DESE are driven by service requests initiated by DESE partners, also referred to as customers, and require the use of messaging and data persistent middleware to service data calls from their respective systems.

DESE is a system of middleware applications that is responsible for the transport of Veterans health, benefits, or administrative data between DESE partners. DESE partners are generally categorized into two groups: producers who typically provide data and can be external or internal to VA; and consumers who are typically partners that are end users of data and are internal or external to VA.

DESE provides a common access mechanism for data related to Veterans' electronic record information which is stored in and outside of VA. The VLER DAS MongoDB is authorized to store 3rd party data (e.g., external Veteran/Service Member data) which is transported from the provider entity (e.g., DoD, Walgreens, contracted vendors) to the large MongoDB repository.

DAS was, and DESE is, essential to VA's ability to execute its mission and proactively provide Veterans with access to the full continuum of services and benefits they have earned. DESE sets the foundation for sharing information within VA and between VA and its external partners. DESE delivers a wide range of integrally linked, complementary capabilities that enable information sharing throughout VA and with its partners.

DESE delivers a wide range of integrally linked, complementary capabilities that enable information sharing throughout VA and with its partners, including but not limited to:

- Affordable Care Act (ACA) Reporting to Centers for Medicare/Medicaid Services (CMS)
- Joint Legacy Viewer (JLV)
- Veteran Health Information Exchange (VHIE) (formerly known as VLER Health) and eHealth Exchange
- VA Pharmacy Re-engineering (PRE) Inbound Prescriptions (eRX)
- Veterans Benefits Management System (VBMS)
- Veterans Health Information Systems and Technology Architecture (VistA) Imaging (VI) Viewers (Computerized Patient Record System [CPRS], JLV,
- Electronic Health Management Platform [eHMP])
- Community Care (Community Care Network)

## 2.0 APPLICABLE DOCUMENTS

1. In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:
2. 44 U.S.C. § 3541-3549, “Federal Information Security Management Act (FISMA) of 2002”
3. “Federal Information Security Modernization Act of 2014”
4. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”
5. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
6. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
7. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
8. 10 U.S.C. § 2224, "Defense Information Assurance Program"
9. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
12. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, https://www.va.gov/vapubs/index.cfm
13. VA Handbook 0710, “Personnel Security and Suitability Program,” May 2, 2016, https://www.va.gov/vapubs/index.cfm
14. VA Directive and Handbook 6102, “Internet/Intranet Services,” August 5, 2019
15. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” January 18, 2017
16. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
17. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
18. NIST SP 800-66 Rev. 1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021
22. VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021
23. 
24. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” March 12, 2019
25. VA Handbook 6500.5, “Incorporating Security and Privacy into the System Development Lifecycle,” March 22, 2010
26. VA Handbook 6500.6, “Contract Security,” March 12, 2010

27. VA Handbook 6500.8, “Information System Contingency Planning,” April 6, 2011
28. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018
29. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
30. OIT Process Asset Library (PAL), https://www.va.gov/process/ . Reference Process Maps at https://www.va.gov/process/maps.asp and Artifact templates at https://www.va.gov/process/artifacts.asp
31. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
32. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
33. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
34. VA Handbook 6510, “VA Identity and Access Management,” January 15, 2016
35. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
36. VA Directive 6300, “Records and Information Management,” September 21, 2018
37. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010
38. NIST SP 800-37 Rev 2, “Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,” December 2018
39. NIST SP 800-53 Rev. 5, “Security and Privacy Controls for Federal Information Systems and Organizations,” September 23, 2020 (includes updates as of 12/10/2020)
40. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
41. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
42. 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
43. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
44. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
45. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011, (NOTE: Part A of the FICAM Roadmap and Implementation Guidance, v2.0, was replaced in 2015 with an updated Architecture (https://arch.idmanagement.gov/#what-is-the-ficam-architecture)
46. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
47. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” updated March 02, 2020
48. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
49. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981, “Mobile, PIV, and Authentication,” March 2014

50. 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)
51. 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)
52. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896
53. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, https://www.cisa.gov/publication/tic-30-core-guidance-documents
54. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
55. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
56. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
57. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
58. Executive Order 13834, “Efficient Federal Operations,” dated May 17, 2018
59. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
60. VA Directive 0058, “VA Green Purchasing Program,” July 19, 2013
61. VA Handbook 0058, “VA Green Purchasing Program,” July 19, 2013
62. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
63. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
64. “Veteran Focused Integration Process (VIP) Guide 4.0,” January 2021, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
65. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
66. “DevSecOps Product Line Management Playbook” version 2.0, May 2021, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946
67. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
68. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
69. Social Security Number (SSN) Fraud Prevention Act of 2017
70. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018
71. FedRAMP Authorization Act, December 23, 2022
72. VA SaaS Definition - Attachment 1
73. Existing VA Enterprise Case Management Solutions (VECMS) Solutions - Attachment 2

Please be advised that any hyperlinks contained within this document, if any, are for convenience purposes, only. Due to the dynamic nature of hyperlinks and the information accessed through or imbedded therein, it is incumbent upon the Contractor to ensure that all information required to successfully complete the requirements established herein is independently located, verified for accuracy, and confirmed to be the most up-to-date version available, prior to use.

## 3.0 SCOPE OF WORK

The Contractor is required to offer a comprehensive range of services for the systems outlined in Sections 1.1 to 1.12. These services include production and non-production support and provisioning, operations and maintenance (O&M) for all product environments, project/product management, solution development, coordination with partners, software integration, testing, release management, technical support, training, content management, systems engineering, development, enhancements, modernization, and documentation. These services should support the Veterans Affairs Office of Information Technology (VA OIT) processes and adhere to the DevOps and agile methodologies. Agile processed and frameworks utilized will vary by team and may include Scrum, Kanban, and the Scaled Agile Framework (SAFe). Some product teams may employ tailored hybrid approach based on the previously listed frameworks and methodologies.

Additionally, the Contractor must adhere to VA 6500 policies, Service Level Agreements (SLAs), and Authority to Operate (ATO) requirements. The contractor may be called upon to facilitate the modernization of legacy applications through transition of hosting to the VAEC cloud environment and will be responsible for proposing solutions that utilize cloud-native, highly resilient design patterns where able. Some modernization efforts may require the adoption of Low Code/No Code (LCNC) solutions built upon approved VA OIT platforms. All modernization and re-hosting efforts will require the Contractor to develop decommissioning plans for legacy environments and must include support for training of VA staff, end users and other technical personnel identified in the planning cycle.

For the Base Period and all Option Periods, the Contractor must provide scrum teams (as detailed in PWS 4.6.1) to support O&M for the products listed in Sections 1.1 through 1.12. Any additional O&M and Development teams needed throughout the task order period will be addressed by authorizing optional tasks for additional scrum teams.

## 3.1 APPLICABILITY

This Task Order (TO) effort PWS is within the scope of paragraph(s) of the T4NG Basic PWS:

> 4.1 Program Management, Strategy, Enterprise Architecture and Planning Support
> 4.1.1 Strategy and Planning

4.1.2 Standards, Policy, Procedure and Process Development, and Implementation Support
4.1.3 Requirements Development and Analysis Support
4.1.3.1 Requirements Packages
4.1.4 Technology Refresh and Configuration Reviews

4.1.5 Studies and Analyses
4.1.6 Program Management Support
4.1.7 Product Data
4.1.8 IT Services Management Support
4.2 Systems/Software Engineering
4.2.1 Design and Development
4.2.2 Architecture Development
4.2.4 Enterprise Application/Services
4.2.5 Cloud Computing
4.2.6 Web Application Design and Development
4.2.7 Mobile Application Design and Development
4.2.8 Human-computer Interaction
4.2.9 System/Software Integration
4.2.10 Modeling and Simulation
4.4.11 Informatics Services
4.2.12 Engineering and Technical Documentation
4.2.13 Current System and Data Migration
4.2.14 Devlopment Toolkit Support
4.3 Software Technology Demonstration and Transition,
4.4 Test and Evaluation (T&E)
4.5 Independent Verification and Validation (IV&V)
4.6 Enterprise Network
4.8 Operations and Maintenance
4.9 Cyber Security
4.10 Training
4.11 Information Technology Facilities.

## 3.2 ORDER TYPE

The effort shall be proposed on a hybrid Firm Fixed Price (FFP) and Time and Materials (T&M) basis with a Cost Reimbursable (CR) line item for travel. The Optional Tasks for Development referenced in PWS Sections 5.5.1 CDW Admin & Support Services, 5.5.3 Build and Development and 5.6 Solution Architect shall be proposed on a T&M basis.

# 4.0 PERFORMANCE DETAILS

## 4.1 PERFORMANCE PERIOD

The Period of Performance (PoP) shall consist of one 12-month base period, four 12-month option periods, and nine Optional Tasks. The overall PoP shall not exceed 60 months.

## 4.2 PLACE OF PERFORMANCE

The work to be performed under this TO shall be performed at Contractor furnished facilities and work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR). Work shall  be conducted during core business hours of 8:00am-5:00pm EST, unless specified otherwise. For specific meeting types, including user requirements sessions and other key meetings which are best accomplished at Government facilities, the Government will schedule meeting rooms as necessary. No work under this TO shall take place outside the United States. If required, all travel will be pre-approved by the COR.

## 4.3 TRAVEL OR SPECIAL REQUIREMENTS

The Government anticipates travel to perform the tasks associated with the effort to attend program-related meetings and user requirement sessions throughout the PoP. Travel shall be proposed on a Cost-Reimbursable basis. There will be 12 large trips of 20 people yearly traveling to DC, Austin, TX, and St. Petersburgh FL, and 40 trips of 4 people or less per year to various US destinations. Travel shall be in accordance with the Federal Travel Regulations (FTR) and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed.

## 4.4 CONTRACT MANAGEMENT

All requirements of Sections 3.0 and 5.0 of the PWS apply to this effort. This TO shall be addressed in the Contractor's Progress, Status and Management Report as set forth in the T4NG Basic contract. (TBD based on RFI)

## 4.5 GOVERNMENT FURNISHED PROPERTY

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

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

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

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

1. Up to 150 developer-grade laptops
2. Up to 250 standard grade laptops.

The Government will not provide IT accessories including, but not limited to Mobile Wi-Fi hotspots/wireless access points, additional or specialized keyboards or mice, laptop bags, extra charging cables, extra Personal Identity Verification (PIV) card readers, peripheral devices, or additional Random Access Memory (RAM). 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.

The Status of Government Furnished Equipment Report under the T4NG Basic Contract requirements is applicable to this TO and shall be delivered to the COR/VA PM as required.

## 4.6 SCRUM TEAM / PERSONNEL REQUIREMENTS

### 4.6.1 SCRUM TEAM SIZE

| Task Size / Complexity | Description |
|---|---|
| Spike | A Spike Scrum Team is appropriate for short, focused activity by individuals with deep experience or specific skills. Spike Teams would be utilized to investigate new technologies, evaluate tools and third-party products for fit within the products/programs they support, or evaluate feasibility of complex architecture changes. |
| Small | System efficiency improvements; minor to moderate changes to existing processes. Updating existing letters, forms, reports or correspondence protocols, and modify API. Moderate to major user interface updates. Modifications/deletions to 3 to 8 data fields in an information service (and |

| Task Size / Complexity | Description |
|---|---|
| | corresponding adapter, access, and/or partner component). Minor user interface changes or API if applicable, reference table updates, data validation, minor updates to existing business rules or existing services, modifications/deletions to 2 or less data fields in an information service (and corresponding adapter), |
| Medium | Minor to moderate enhancements, major business rule additions or rewrites, extensive database modifications or major modifications to existing services, new letters, forms, reports, or correspondence protocols, 1-2 new SOA components (Presentation, Process, Information, Business Application, Access, Partner, Infrastructure levels), integration with new system, system modifications to propagate/seed/synchronize authoritative data to/from a source where a propagation or seeding exists. Orchestrations with 1-2 non- dependencies. Additions / modifications / deletions to 9 data fields in an information service (and corresponding adapter, access, and/or partner component), Development of new web services requiring 1-2 component levels. |
| Large | Development of new web services or APIs requiring 3-5 or more component (logic layer, service layer, infrastructure layer, or partner layer) levels, or extensive system modifications to propagate/seed/synchronize authoritative data to/from a new service, orchestrations with 3-5 dependencies. Development of new web services or APIs requiring 5 or more component levels and 2+ integrations, orchestrations with 6 or more dependencies, major system enhancements impacting multiple systems/services. |
| Multi | Multi-Team: The Contractor shall provide a combined scrum team consisting of a minimum of 12 FTE and a maximum of 18 FTE resources in total led by a single scrum master to support all services/deliverables required by PWS 5.2 (O&M), PWS 5.3 (CDW Support), PWS 5.4 (VINCI Support) or PWS 5.5 (Development), including all subparagraphs |

.

### 4.6.2 Personnel Requirements

The Contractor shall provide at least one Scrum Alliance Certified Scrum Master for every two active scrum teams.

The Contractor shall provide personnel with requisite skillsets to support the following functional areas for all products:

- Application/System Support – Tier 3 fault isolation and triage
- Database Administration, Operations and Development
- Application/System Administration
- Application/Systems Engineering
- Software Development

- Middleware Support
- Monitoring Tools Support
- Integration of Commercial Off the Self
- Technical requirements analysis
- Technical writing
- Test, evaluation and reporting
- Security analysis and support
- Data and Systems Architecture
- Extract, Translate and Load (ETL) Engineers
- Lakehouse Pattern Data Engineers
- RPA Engineer

For each specific product, the Contractor shall provide personnel with expertise in the following implementation patterns, technologies, and methodologies:

**VIERS:**

- Examples of the Tools/Dependencies used in the VIERS Application are:
  - IBM App Connect Enterprise (ACE) Enterprise Service Bus (ESB) Licenses
  - Oracle WebLogic
  - RESTful and SOAP Services
  - Java
  - Ready API Test
  - Oracle
  - SQL
  - GitHub
  - AWS cloud admin tool sets
  - Linux

- The contractor shall have demonstrable subject matter expertise in the following implementation patterns, technologies, and methodologies to provide required maintenance and enhancements to the VIERS system.
  - End Point Code incrementing in the VBA environment.
  - Bridging between WebLogic and WebSphere Message Brokers to include configuring batch sizes.
  - Defining Extensible Markup Language (XML) namespace to enable WebSphere processing.
  - Establishing clustered singletons to manage polling services.
  - Implementing and maintaining manifests to support management of XML messages in an asynchronous process.
    - Using VistA Link libraries for web service calls.

- Message queuing and retry techniques after message failure in a multi-broker (WebSphere and WebLogic) environment.
- Bindings when using dynamic Web Services Description Language (WSDL) returns in a reverse proxy environment using Apache and WebLogic.
- Record locking techniques in a clustered, singleton configuration.
- Using Introscope workbench features to monitor across a SOA stack. Use of Express Persistent Objects (XPO) Log.
- The Contractor shall provide Operations and Maintenance (O&M) support for all VIERS Suite of Systems and applications.

**DAS:**

- Tools/Dependencies
    - Apache CXF, 3.2.x
    - Apache Maven, 3.5.x
    - AWS API Gateway
    - AWS API Gateway
    - AWS Cloud Formation
    - AWS CloudTrail
    - AWS CloudWatch
    - AWS Elastic Load Balancer
    - AWS ElastiCache
    - AWS Glacier
    - AWS Lambda
    - CentOS (Development), 7.x
    - Docker, 17.12
    - Elastic Compute Cloud (EC2)
    - Git, 2.1.4
    - HP Fortify, 17.2
    - Java SE, 1.8
    - Jenkins Server, 2.150.1
    - Jetty, 9.4
    - Junit,4.12
    - McAfee MWG Appliance, 7.x
    - Mocha, 2.0.1
    - MongoDB Enterprise, 3.6
    - MongoDB Ops-Manager, 3.6
    - Node npm, 4.4.4
    - Node.js Express, 4.16.x
    - Node.js Restify, 5.2
    - Node.js, 10.x
    - OpenShift Enterprise, 3.11
    - Oracle Java 8, 1.8
    - OWASP Enterprise Security API, 2.1
    - Prometheus, 2.x
    - Python, 2.7
    - Rational Team Concert, 2.1.4
    - Ready API/LOAD UI, 2.2
    - RedHat 3Scale, 2.4
    - RedHat Ansible Tower, 3.4.x
    - RedHat Enterprise Linux, 7.x
    - RedHat OpenShift, 3.11
    - Ruby on Rails, 2.5.x
    - SOAP UI, 5.x
    - Sonatype Nexus Server, 3.15.1
    - Spring Framework, 5.x
    - VirtualBox, 6.0.4
    - Weblogic JMS, 12.2
    - Weblogic, 12.2
    - Windows 10 Enterprise, 10

**HDR**

- Tools / dependencies:
  - 7-Zip
  - Apache Ant
  - Apache Commons BeanUtils
  - Apache Commons Collections
  - Apache Commons Database Connection Pooling (DBCP)
  - Apache Commons Digester
  - Apache Commons Lang
  - Apache Commons Logging
  - Apache Commons Pool
  - Apache CXF
  - Apache MINA
  - Apache Tomcat
  - AppDynamics
  - AspectJ
  - Aspect-Oriented Programming (AOP) Alliance
  - Attachmate Reflections
  - Attachmate Reflections X Advantage
  - Cache InterSystems
  - Confluence
  - Cygwin
  - dom4j
  - Easymock
  - Eclipse
  - Firefox
  - Fortify
  - Hermes JMS
  - Hibernate ORM
  - HL7 HAPI
  - HTTP/HTTPS
  - Intuitive Reliable Interoperative Scalable (IRIS) for Health
  - Java Development Kit (JDK)
  - Java JAXB
  - Java SE
  - JSON in Java
  - Jenkins
  - Jira
  - Junit
  - Linux
  - Log4j
  - Maven
  - Mockito
  - MS Project
  - MS SQL Server Management Studio
  - MUMPS
  - Nexus
  - Notepad
  - Notepad++
  - Oracle Advanced Compression
  - Oracle Automatic Storage Management
  - Oracle Client
  - Oracle Database
  - Oracle Enterprise Manager
  - Oracle Golden Gate
  - Oracle RDBMS
  - Oracle Real Application Clusters
  - Oracle Solaris
  - Oracle SQL Developer
  - Powermock
  - Putty-CAC
  - Quartz
  - Red Hat Enterprise Linux (RHEL)
  - Saxon
  - SLF4j
  - SoapUI
  - SonarQube
  - Splunk Enterprise
  - Spring Framework
  - SharePoint
  - SQL
  - Toad Data Modeler
  - Toad for Oracle
  - Unix Solaris
  - VirtualBox
  - Weblogic Server
  - Windows Remote Server Administration Tools/Windows AdminPack &
  - Windows Server
  - WinSCP
  - WinZip
  - Xerces2
  - XML
  - XMLSpy
  - xRDP
  - XSLT

**VADIR/VIS**

| Software Component | Version In-Use | TRM Allowed Versions | TRM Link | Comments |
|---|---|---|---|---|
| Apache HTTP Server | 2.4.6 | 2.4.6 (No Expiration) | Apache Hypertext Transfer Protocol (HTTP) Server (va.gov) | |
| AppDynamics Agent | 23.2 | 23.x (Approved) | AppDynamics (va.gov) | Dependency on VA Enterprise monitoring version |
| AZCopy | | 10.1.x (Unapproved)<br>10.5.x (Divest Q2-24)<br>10.16.x (Approved) | Microsoft AzCopy (va.gov) | Dependency on CxDW version |
| connectDirect | 6.1 | 6.1.x (Divest Q1-24)<br>6.2.x (Approved) | International Business Machine (IBM) Sterling Connect:Direct (va.gov) | Dependency on Prudential, Hines versions |

| | | | | |
|---|---|---|---|---|
| Java Development Kit | **OGG 1.8.0_351**<br>**TRF 1.8.0_351**<br>**SYM 1.8.0_351**<br>**APP 1.8.0_371** | 1.8.0_351 (Unapproved)<br>1.8.0_361 (Unapproved)<br>1.8.0_371 (Divest Q3-23)<br>1.8.0_381 (Approved Q4-23) | JDK - Oracle Java Standard Edition (SE) Development Kit | |
| Jetty | 9.4.44 | 9.4.x (Approved) | Jetty (va.gov) | |
| Oracle GoldenGate | 21.9 | 19.x (Divest Q3-23)<br>21.x (Approved) | Oracle GoldenGate (va.gov) | |
| Oracle RDBMS | 19c | 19.x (Approved) | Oracle Database (va.gov) | |
| Oracle Weblogic | 12.2.1.4 | 12.2.x (Approved)<br>14.1.x (Approved) | WebLogic Server (va.gov) | |

| | | | | |
|---|---|---|---|---|
| RedHat Linux | 7.9 | 7.x (Divest - No expire)<br>8.x (Approved) | Red Hat Enterprise Linux (RHEL) (va.gov) | Current research underway to update to 8.x |
| Symmetric DS | 3.12.19 | 3.12.x (Divest Q1-24)<br>3.14.x (Approved) | JumpMind SymmetricDS (va.gov) | |

**VA Profile:**

- Tools / dependencies:
- AL2
- Apache HTTP Server
- Confluence
- Corretto Open JDK
- Cucumber
- Databricks
- Docker
- ElasticCache
- Open Search
- Eureka
- Fortify
- GoldenGate
- Grafana
- HAProxy
- Hibernate ORM
- Hystrix
- Jenkins
- Jira
- JMeter
- JUnit
- Kafka
- Kubernetes (EKS)
- Liquibase
- Logstash
- Maven
- Nexus
- Oracle RDBMS
- PowerBI
- Prometheus
- Rancher
- Red Hat Linux
- REST
- SonarQube
- Spectrum Platform
- Spring Boot
- Spring Cloud Config
- Spring Cloud Gateway
- Spring Cloud Stash
- Spring Framework
- Spring Security
- Swagger
- Toad
- Tomcat
- Vault

- zipkin
- zipkin-dependencies
- Zookeeper
- Zuul
- Amazon Secrets Manager

- Patterns / implementation methodologies:
    - Change data capture synchronization pattern using Oracle GoldenGate
    - Service based synchronization pattern using RESTful services
    - Domain drive microservice pattern
    - Circuit breaker pattern
    - Behavior driven development (BDD)

**CDW:**

Tools / dependencies:

- SQL Server
- Oracle
- Solarwinds
- System Center Operation Manager (SCOM)
- GitHub
- SQL Server Tool Suite (SSIS, SSAS)
- Pyramid Analytics version 6 or later
- On Line Analytical Processing (OLAP) cubes
- Data Domain ETL Script Implementation Document SSAS 2014 (or later)
- PowerBI

**VINCI:**

Tools / dependencies:

- HP Storage Essentials
- HP Report Optimizer
- Systems, Application and Products Exchange Infrastructure (SAP XI)
- Crystal Reports
- HP 3PAR Performance & Reports Manager
- Solarwinds
- HP Insight Remote Support
- HP B-Series SAN Network Advisor
- HP P6000 and EVA Performance Data Collector.AL2
- Microsoft Data Protector Manager
- HP Data Protector
- Commvault
- Linux SAS 9.X
- Hadoop 3.X

- Red Hat Enterprise Linux (RHEL) and CentOS versions 6.x and 7.x
- Microsoft Forefront Threat Management Gateway

**RPA:**

Skillsets / Services:

- Robotic Process Automation System Administration (RPA), Operations and Maintenance (UIPath and Blue Prism)
- RPA Development
- RPA Automation Operations and Maintenance

Tools / dependencies

- Blue Prism
- UIPath
- Azure Cloud Services
- Azure Virtual Network
- Azure Virtual Machines
- Azure Monitor
- Azure Storage Accounts
- Azure SQL Database
- Azure Load Balancer
- Azure Log Analytics Workspaces
- Dynatrace
- Microsoft Office Word
- Microsoft Office Excel
- Microsoft Office Outlook
- Microsoft GraphAPI
- Azure Kubernetes (AKS)
- GitHub
- kubectl
- Power BI
- MS SQL Server Integration Services
- CyberArk

## 4.7 SECURITY AND PRIVACY

All requirements in Section 6.0 apply to this effort. Specific TO requirements relating to Addendum B, Section B4.0 paragraphs j and k supersede the corresponding T4NG Basic PWS paragraphs, and are as follows:

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 on the severity of the incident.

It has been determined that protected health information may be disclosed or accessed, and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, attached to the Request for Task Execution Plan (RTEP) and shall comply with VA Directive 6066.

### 4.7.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

**Position Sensitivity and Background Investigation Requirements by Task**

| Task Number | Tier1 / Low Risk | Tier 2 / Moderate Risk | Tier 4 / High Risk |
|---|---|---|---|
| 5.1 | □ | ☒ | □ |
| 5.2 | □ | ☒ | □ |
| 5.3 | □ | ☒ | □ |
| 5.4 | □ | ☒ | □ |
| 5.5 | □ | ☒ | □ |
| 5.6 | □ | ☒ | □ |
| 5.7 | □ | ☒ | □ |
| 5.8 | □ | ☒ | □ |
| 5.9 | □ | ☒ | □ |
| 5.10 | □ | ☒ | □ |
| 5.11 | □ | ☒ | □ |
| 5.12 | □ | ☒ | □ |
| 5.13 | □ | ☒ | □ |

The Tasks identified in the above table 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.

## 5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor is tasked with supplying the necessary resources for designing, configuring, developing, integrating, and implementing solutions based upon open, flexible and scalable architectures reflective of the state of the industry. This approach aims to provide the VA with modern, lower-complexity, modular solutions that are built upon cloud-native services where possible and minimize vendor lock-in. Proposed and implemented architectures may utilize Platform as a Service (PaaS) capabilities to minimize complexity, Software as a Service (SaaS) integrations, APIs for integrations with partner/external systems, and support emerging digital modernization technologies. Compliance with the latest VA Directives, Policies, Guidebooks, and applicable Federal Regulations is required.

Integration and development of each product/platform will adhere to a unified Software Development Life Cycle (SDLC) process where able that is in line with VA Product Line Management (PLM) standards and OI&T engineering and release management directives. All stages of analysis, design, construction, testing, and deployment, along with associated documentation, must follow these guidelines. Proposed solutions, lifecycle processes and designs may be subject to review through the PES DA Architecture review Council.

The Contractor is expected to support VA’s continued adoption of principles that enable IT as a product. This includes integration of product thinking concepts to all aspects of the planning, development and delivery process including product planning activities such as backlog grooming and prioritization throughout each product’s life cycle.

## 5.1 PROJECT MANAGEMENT (FFP)

### 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 initial baseline CPMP shall be concurred upon and updated in accordance with Section B of the TO. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP.

**Deliverable:**

A. Contractor Project Management Plan

### 5.1.2 TECHNICAL KICKOFF MEETING

A technical kickoff meeting shall be held within 10 days after TO award. The Contractor shall coordinate the date, time, and location (can be virtual) with the Contracting Officer (CO), as the Post-Award Conference Chairperson, the VA PM, as the Co-Chairperson, the Contract Specialist (CS), and the COR. The Contractor shall provide a draft agenda (via email) to the CO, CS, COR, and VA PM at least five (5) calendar days prior to the meeting. Upon Government approval of a final agenda, the Contractor shall distribute to all meeting attendees). During the kickoff-meeting, 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 via a Microsoft Office PowerPoint presentation. At the conclusion of the meeting, the Contractor shall update the presentation with a final slide entitled "Summary Report" which shall include notes on any major issues, agreements, or disagreements discussed during the kickoff meeting and the following statement "As the Post-Award Conference Chairperson, I have reviewed the entirety of this presentation and assert that it is an accurate representation and summary of the discussions held during the Technical Kickoff Meeting for the <insert title of effort>,". The Contractor shall submit the final updated presentation to the CO for review and signature within three (3) calendar days after the meeting. The Contractor shall also work with the CS, the Government's designated note taker, to prepare and distribute the meeting minutes of the kickoff meeting a to the CO, COR and all attendees within three (3) calendar days after the meeting. The Contractor shall obtain concurrence from the CS on the content of the meeting minutes prior to distribution of the document.

Deliverables:

A. Draft Agenda
B. Final Agenda
C. Kickoff Meeting Power Point Presentation
D. Meeting Minutes

### 5.1.3 ONBOARDING STATUS (FFP)

The Contractor shall manage the onboarding of its staff on this TO. 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, test and/or production environments for the various systems to be enhanced. After review between the Contractor and VA COR(s), 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 Point of Contact (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(s). All VA onboarding paperwork shall be stored on the deliverables folder in the COR designated VA SharePoint site or equivalent tool. 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 for any staff with outstanding onboarding requests in the bi-Weekly Status Report (5.1.5).

**Deliverables:**

A. Weekly Onboarding Status Report

### 5.1.4 PRIVACY, HIPAA, AND ELEVATED PRIVILEGES TRAINING (FFP)

The Contractor shall submit Talent Management System (TMS) training certificates of completion for VA Privacy and Information Security Awareness and Rules of Behavior and Health Insurance Portability and Accountability Act (HIPAA) training and 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 provide a copy of the Privacy, HIPAA and Elevated Privileges Training Roster to indicate the staff that have and have not completed the training in the Monthly Status Report (5.1.5).

**Deliverables:**

A. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate
B. Signed Contractor Rules of Behavior
C. VA Health Insurance Portability and Accountability Act (HIPAA) Training Certificate

### 5.1.5 REPORTING REQUIREMENTS (FFP)

The Contractor shall provide the COR with a Bi-weekly Status Report using a modern, automated tool. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. The report shall reflect data as of the last business day of the preceding period. The Progress Report shall cover all work completed during the reporting period and work planned for the subsequent reporting period for each project. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The report shall also include an itemized list of all documents and electronic deliverables. The Contractor shall monitor performance against the VA PARS/CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues. The Contractor shall also provide the data and reporting content to support management level reporting.

The Contractor shall show all Agile requirements, changes, tests performed and test results in approved project management tools (i.e., JIRA) to show evidence of code coverage and test coverage of all the requirements specified. This expectation will allow VA to have high confidence in a fully documented, as evidenced by data in the tools, requirements traceability matrix.

The Contractor shall track all risks in the VA approved project management tool utilized by the team they are supporting. This could include Jira, MS Project or other industry standard tools. Risk identification should include impact statements including severity, likelihood of impact and a proposed mitigation strategy. Risk status should be reviewed an updated at least once per week. Risks that are impactful to the product, the Pillar or Portfolio should be documented in the associated VA PARS entry for the product/program.

Additionally, the Contractor shall produce a Partner Integration Report that identifies Partner Systems that interface with each product. Partners are other VA OI&T Product Teams and external consumers that integrate with products/platforms supported by the Contractor  This report shall include a summary description of each interface, current issues, planned updates, changes in status, impact to the partner if unavailable and dependencies with each Product. The initial copy of this report shall be delivered electronically within (90) days of TO award and updated electronically for every sprint thereafter.

**Deliverable:**

A. Bi-weekly Status Report
B. Partner Integration Report

### 5.1.6 OFFBOARDING STATUS (FFP)

The Contractor shall manage the offboarding process for VA access and to individual system/environment access for all project management, core team, development, and O&M Contractor staff. The Contractor shall prepare all forms necessary for termination of access to VA information systems, in accordance with VA guidance. The Contractor shall assist in confirming whether the GFE equipment, associated documentation, and PIV card has been returned to the proper receiving authorities in accordance with VA policy. The Contractor shall provide an Offboarding Status Report for any staff with outstanding offboarding requests in the Bi-Weekly Status Report (5.1.5). COR notification of fully offboarding Contractor shall be provided within (24) hours of terminated employment clearly demonstrating all access and permissions have been disconnected.

### 5.1.7 CONFIGURATION MANAGEMENT (FFP)

The Contractor shall update the Configuration Management Plan as required to reflect these requirements:

1. Identify the standard and unique aspects of Product Configuration Management (CM) to be performed for each product by establishing a Product Configuration Management Plan which meets PES 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.

2. Deliver a Recommended List of Configuration Items to include documents, technical stories, compiled and uncompiled software, libraries, diagrams, and models to be placed under configuration and change control in the Configuration Management Plan (CMP). The Contractor shall identify types of configuration items pertaining to each product to be placed under configuration management. Based on PES 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.

3. Use GitHub or other VA specified tool and repository for all software source code and electronic artifact configuration and version management. The Contractor shall use JIRA and

the specified tool to manage change, activity, issue, action, risk, and other project data as prescribed by VA standards and processes. If assigned a project using tools that are being deprecated, the Contractor shall assist the VA Tools Team in migrating data from projects using other Change and/or Configuration Management tools to the specified tool and repository.

4. Ensuring that every item approved for configuration control, including software, is stored and managed within the VA specified tool. The Contractor shall check-in every update to items daily. Ensure that all project software and non-software artifacts are versioned correctly according to VA standards and follow a build/release promotion versioning approach which identifies all major, minor, and update changes to the components.

5. Create Project and Product Artifacts baselined and versioned in the CM repository to allow the tool to show active and past histories of the check-ins and check-outs of all software components, data, and software project engineering documents. Maintain all baselines of software, software builds, and electronic artifacts in the repository, labeling updates and versions according to CM procedures.

6. Develop, verify, and submit with all project build deliveries, a Version Description Document (VDD) and System Design Document (SDD), in accordance with Section 5.3 that conforms to PES Website standard templates and addresses the manifest of the contents of all software builds created for project releases outside the development environment.

7. Establish and maintain status reporting on change and configuration management activity and ensure the VA approved tool data records and artifacts are filed and updated daily.

8. Describe within CMP, how changes are identified and processed against configuration-controlled items.

9. Coordinate the schedule for all product releases via Change Request in Service Now. Releases shall be executed following approved VA processes.

10. Describe method for code promotion between environments.

11. Describe processes for creating automated builds.

**Deliverables:**

A. Product Configuration Management Plan Semi-Annually
B. VDD and SDD with every major release

### 5.1.8 SCHEDULE MANAGEMENT (FFP)

The Contractor semimonthly and ad hoc, shall create, maintain, analyze, and report integrated schedules for VA products. The Contractor shall provide schedule updates as directed by the VA Government PM and using approved VA tools.

**Deliverables:**

A. Semi-Monthly and Ad Hoc Schedules

### 5.1.9 RISK MANAGEMENT (FFP)

The Contractor shall conduct risk management of all work performed under this TO and provide input to the Product Risk Registry. Contractor should categorize impact statement and deliver within 24 hours of incident.

**Deliverables:**

A. Product Risk Registry

### 5.1.10 INCIDENT REPORTING (FFP)

The Contractor shall report any incidents or outages that may occur in the course of all work performed under this TO. Such reporting shall conform to standards of the Incident Management team. The Contractor shall supply a weekly Executive Summary which includes cumulative reporting of incidents or outages to the VA team that shall include, at a minimum, a summary of the incident, its root cause, recovery actions and corrective actions to be taken to prevent a future occurrence. Root Cause Analysis (RCA) and After-Action Report (AAR) shall be delivered within (1) business day after the closure of the reported outage or incident.

**Deliverables:**

A. Weekly Incident Executive Summary
B. Root Cause Analysis and After-Action Report

## 5.2 OPERATIONS AND MAINTENANCE (FFP)

This task includes sustainment of the current product environments during the period of performance for:

**Table 1 Mission Criticality**

| Product | Platform | Mission Level |
|---|---|---|
| VA DoD Identity Repository (VADIR) | VAEC (AWS Cloud) | Critical |
| VA Profile | VAEC (AWS Cloud) | Critical |
| Veterans Information Solution (VIS) | VAEC (AWS Cloud) | Critical |
| Veteran Identity/Eligibility Reporting System (VIERS) | VAEC (AWS Cloud) | Routine |
| Health Data Repository (HDR) | AITC | Critical |
| Corporate Data Warehouse (CDW) | AITC | Critical |
| Summit Data Platform (SDP) | VAEC Cloud (Azure) | Critical |
| Customer Insights (CxDW) – Hosted by SDP | VAEC (Azure Cloud) | Critical |

| | | |
|---|---|---|
| VA Informatics & Computing Infrastructure (VINCI) | AITC | Routine |
| Administrative Data Repository (ADR) | VAEC (AWS) | Critical |
| Robotic Processing Automation (RPA) Platform | VAEC (Azure) | Routine |
| Data Access Services (DAS) | VAEC (AWS Cloud) | Critical |
| Data Interoperability (DI) | SAAS | Routine |
| Health Data Analytics Platform (HDAP)- Hosted by SDP | VAEC (Azure Cloud) | Critical |

The Contractor shall provide support for all technologies of these systems (or other appropriate PES DA Products, based upon exercise of Operations and Maintenance Services and the appropriate O&M Support Optional Tasks paragraph 5.5 and associated sub-paragraphs) identified in Section 4.6 above.

Technologies for additional Programs and Projects identified in Section 4.6 will be supported as Optional Tasks awarded under this TO. Operations and Maintenance System solution support activities are associated with the ongoing support related to the performance of routine, scheduled, adaptive, preventive, predictive, and unscheduled actions aimed at preventing system/production failure (i.e., break/fix) and correcting software defects with the goal of increasing efficiency and reliability on a continuous basis.

Periodic maintenance - The Contractor shall plan for and perform routine and/or periodic maintenance on all applications/systems supported within the first (30) days post base and option year awards. The Contractor shall be responsive to ad hoc compliancy audits and remediate any defects found thereby in accordance with defect processing. The Contractor shall make documentation updates based upon periodic maintenance activities monthly.

Enhancements– Contractor shall address modifications to applications/systems to cope with changes in the software environment. For example, software, databases, or documentation adjustments required as a result of scheduled minor hardware, software, and infrastructure updates or tech refreshes. This extends to standards evolution for existing compliancy requirements (such as IPv6, 508 compliance, etc.), Congressional mandates, and changes in business rules or procedures external to the product. The Contractor shall perform all such remediation of defects found thereby in accordance with defect remediation processing.

The Contractor shall perform operations and maintenance support on existing code and systems that are hosted at either AITC or VA cloud facilities. This may include code developed outside of this TO that integrates with one of the PES DA systems. Contractor will be required to maintain any code, product integrations or other developed solution utilize by the product/program they are providing operations and maintenance services. Sustainment tasks include production maintenance, environment management, help desk support/escalation, monitoring/logging to ensure system availability, reliability and sustainability.

The Contractor shall use emerging software industry best practices approaches and VA approved tools to facilitate Continuous Development, Continuous Integration (CD/CI), continuous coordination and the continuous sharing of knowledge between development and sustainment teams.

During the O&M phase, the PES DA information system's availability and performance in executing the work for which it was designed shall be maintained.

### 5.2.1 PRODUCTION OPERATIONS SUPPORT (FFP)

Production Support tasks are Help Desk and Tier 2 & Tier 3 support. This includes defect intake from ServiceNow (SNOW), which may consist of, but not limited to: receiving incidents and requests from end-users, analyzing the incidents and requests, and responding to the end-user with a solution or escalation. The production support tasks include support for each product in a production environment.

#### PRODUCTION SUPPORT TIERS

Table 2 Response Tiers

| Tier 1 – Basic | Tier 2 - Intermediate | Tier 3 - Expert |
|---|---|---|
| Initial user point of contact | Major Responsibility: onsite installations or replacements of hardware components, software repair, diagnostic testing, and the utilization of remote-control tools used to take over user's machine for sole purpose of troubleshooting and finding a solution to the problem. | Responsible for the research and development of solutions to new or unknown issues. |
| initial user support | Assist Tier I personnel solving basic technical problems. More knowledgeable on particular product or service than Level I support | Responsible for assisting both Tier I and Tier II personnel. |

#### PRODUCTION OPERATIONS

The Contractor shall provide operational support to keep the production systems and all environments within the accredited boundaries of the ATO in an operational state. This includes supporting the daily uptime of the application/system hardware and operations but also after-hours support during off business hours.

#### MONITORING/MAINTENANCE ACTIVITIES

Support shall be provided 24/7, by Tier 2 and 3. Standby support or on call is acceptable after core hours, as applicable in accordance with the Product's Service Level Agreement (SLA).

The Contactor shall perform software releases including weekends (day and potentially night-time hours) and monitoring/maintenance activities as specified below. VA estimates that regularly scheduled releases will occur twice a month per product. The Contractor shall perform ad hoc emergency releases.

## PRODUCTION SUPPORT

Production Operations are tasks in support of deployment, release, and configuration during sustainment of normal activities and services for the product applications in production. Examples of functions performed by the Contractor shall include Release Management, Configuration Management, and Partner Coordination.

The Contractor shall:

1. Conduct proactive system health monitoring and report any system outage or degradation to the Product Manager COR/PM within one (1) hour of notification for mission critical systems and four (4) hours of notification for non-mission critical systems. Report defects submitted by customers within 48 hours in SNOW.
    A. Mission Critical Data and Analytics Programs: as defined in Section 5.2 above.
2. Develop and deliver configuration, setup, and requirements for services, portlets, Uniform Resource Locators (URLs), and for resolving application and connectivity issues related to the product applications, interfaces, and changes in production.
3. Manage all release activities in accordance with Agile Management guidance and Alignment Epics and User Stories using VA approved tools.
4. Adhere to/with all VA-governing bodies to receive approval for production deployments of the products.
5. Schedule all product releases in accordance with VA approved tools such as: SNOW, Teams, JIRA and VA PARS and track and coordinate license and account renewals.
6. Deploy the configuration control items. Deployment shall be executed following version control processes, including merging, branching, and other activities so that promotion of code and management of configuration items and build versions in all environments are successful. Deployments shall be automated whenever possible to ensure environment configurations and build versions are consistent.
7. Coordinate schedule with the host data center or Cloud Operations staff with patching and maintenance in adherence with VA security compliance to ensure minimal downtime.
8. Monitor deployments for products and all partners across the test sites and the enterprise, and ensure all service level agreement (SLA) requirements are met as defined by each applicable product program where applicable.
9. Provide analysis on continuous improvement of delivery based on retrospectives, lessons learned, trending, and customer site surveys.
10. Identify and triage all reported production problems to the COR/PM, correct any defect or error detected in any deployed component or application. The Contractor shall repair all defects identified in production and follow break fix processes as defined by the COR/PM for repairing production code.
11. Support all operational aspects for code rollbacks to ensure that if any problems are encountered the sustainment team members shall be able to revert to the prior code base or revise code set as directed by Project Manager.

12. Proactively monitor and report capacity issues to the COR/PM according to the Capacity Management Plan thresholds.
13. Monitor the resource consumption trends of current services and their operations, including proactively working with partner systems to understand trends and planned batch events. Tailor resources for scalable responses to these changes without minimal project functionality degradation or lowered response times.
14. Ensure performance for each product is optimized in accordance with the product SLA and its level of criticality.
15. Complete operational analysis related to data issues, including development of data queries, to identify data inconsistency patterns. Queries shall be developed, maintained, and executed in a recurring pattern to identify data-related issues. Reports from query results are shared and reported with the VA PM. Contractor will notify PM of anomalous data mismatches/trends or irregular volume/patterns within (24) hours and make recommendations to remediate within (2) business days of identification.
16. Coordinate with the COR/PM and Host Data Center or Cloud operations to optimize system monitoring and metric reporting in accordance with SLA as defined by each product.
17. Utilize VA provided tools that allow for automated build and automated publishing capabilities to support agile development and continuous integration for every sprint.
18. Assess the as-is system resources for each product (computational, database, networking, etc.). Document and recommend improvements to each system (right size).
19. Support the COR/PM by identifying configuration parameters, setup, and requirements for services, and URLs in the development and testing environment.
20. Respond to production critical and emergency production incidents within (15) minutes 24x7 to support Tier 2 and 3 troubleshooting and resolution of issues related to applications, interfaces, and changes in production of a reported outage.
21. Coordinate with the COR/PM in executing backups.
22. Coordinate with Infrastructure Support Provider (ISP) to ensure all installed monitors are performing per specifications on a 24X7 basis. Notify the Project Manager within 15 minutes of any observed operational issues with monitors on mission critical products and within (3) hours for non-mission critical products.
23. Coordinate with the COR/PM to analyze alerts in near real time - as they are generated. The Contractor is responsible for monitoring and alerting on performance issues at all times. The Contractor shall report discrepancies in the capacity and performance of products in operations to the VA COR/PM.
24. Report and monitor any downstream dependent system outages and provide an impact system to be used for partner notifications.
25. Review and understand the impact of partner integration documents such as Interface Control Documents (ICDs) to better support specific partner interfaces.
26. Complete operational analysis related to data issues, including development of data queries, to identify data inconsistency patterns. Queries shall be developed, maintained, and executed in a recurring pattern to identify data-related issues. Reports from query results are shared and reported with the VA PM and ISSO. Database queries are logged and managed by each Product’s helpdesk and maintained in TRM-approved ticket tracking tools. Notify PM of

anomalous data mismatches/trends or irregular volume/patterns within (24) hours and make recommendations to remediate within (2) business days of identification.

## CONTINUITY OF OPERATIONS AND DISASTER RECOVERY (FFP)

Continuity of Operations and Disaster Recovery (COOP/DR) are the processes and procedures put in place to ensure that all product functions continue during and after a major planned outage, a disaster or national emergency, or some other unanticipated disruption. COOP and DR plans are authored by ISP with input from the PM and the architects. The Contractor shall comply with COOP/DR requirements for all products.

The Contractor shall:

1. Implement VA-architected COOP/DR designs that maximize High-Availability (zero downtime patching) whenever possible for all systems.
2. On an annual basis, the Contractor shall coordinate a scheduled test of COOP and DR environments for automatic failover. Full testing report and outcomes /lessons learned and recommendations for improvement will be made to the Project Manager and the COR within three (3) days of conducting the test. Tests will be repeated until a successful result is achieved.

**Deliverable:**

A. Test Reports, DR Plan, Recommendations and Outcomes

## CONTINUOUS INTEGRATION (FFP)

The Contractor shall:

1. Create a self-testing build and commit new code to the mainline (baseline) at a minimum every day, and during every sprint. If the build is not successful, the Contractor shall resolve all issues. This shall include all activities required to roll back to known, stable code and restore normal operations of the portals and features.
2. Develop and/or maintain an environment for automated builds and the testing of builds. Testing of builds shall include the validation of compiled code and check-ins. Self-testing builds shall include fully-automated and partially-automated test scripts.
3. Verify each build in VA-approved, non-production environments. Each product may have from three (3) to nine (9) non-production environments.
4. Follow the standardized Code Promotion Process as defined in the Configuration Management Plan.
5. Support continuous integration - Develop and deliver a Continuous Integration Plan that ensures early warning of broken/incompatible code and early warning of conflicting changes, including immediate unit testing of all changes.
6. Support continuous integration for rollbacks to ensure that when unit tests fail, or a bug emerges, developers shall be able revert the codebase.

7. VA-approved Code Analysis tools (Sonarqube, CodeQL, Fortify, etc.) shall be executed in the code repository and during the development process, at the time of the automated build, ensuring security and code quality issues are addressed within a sprint.
8. Validate automated testing and tracking of the content for each release through work items and tickets in an issue/defect tracking system approved by the VA COR/PM during development process.

Deliverables:

A. Continuous Integration Plan (Quarterly)

B. VDD

**SYSTEMS ADMINISTRATION (FFP)**

The Contractor shall support IT hardware at the hosting center or Cloud. Includes operating systems, software installation, monitor and optimize system performance, patch, manage security updates and service packs, repair and upgrade IT product software and hardware.

The Contractor shall monitor system resources such as processor, memory and disk utilization using VA approved automated monitoring tools, monitor system logs, create system backups, schedules and tape allocation, establish/maintain access authorizations, perform installations, upgrades or replacements as required.

The Contractor shall receive issues and report resolution progress using approved VA tools (e.g., . ServiceNow, Jira or other similar tools).

For products that utilize a microservice architecture, the Contractor shall manage and monitor container and cluster configurations.

The Contractor shall:

1. Perform initial analysis and triage of complex, high-level activities, including root cause analysis (RCA) for tasks related to troubleshooting Web, App, and Data Server(s), including tasks for log analysis, trend analysis, and patterns that might compromise data.
2. Manage, intake, report, and resolve incidents as they occur, to a high trend predicted to be 15-20 data incidents a week, for each Product. Incident management shall include triage, analysis, root cause, and resolution for each data incident.
3. Manage, intake, coordinate, analyze, report and triage issues. Contractor shall complete analysis, trend pattern reviews, and RCA, and provide recommended solutions to prevent and correct issues.
4. For production support, help desk tickets and data triage:
   a. Determine root cause in missing or mismatched data causing features to not function.
   b. Execute high-level, complex, data integrity analysis.
   c. Determine if the ticket is due to data issues.
   d. When a ticket is identified as a data issue, apply the current data correction process.

   e. Forward information for resolution to the identified data correction authority.
   f. Meet weekly to improve processes, check, and update the status of data corrections.
   g. When the data issue is corrected, contact the customer to verify correction.
   h. Support triage status, tasks, and escalation on tickets.
5. Develop analysis processes and fraud pattern analysis, identifying users and population in portals, to identify possible threats for fraud and data compromise. Notify PM of anomalous data mismatches/trends or irregular volume/patterns within (24) hours and make recommendations to remediate within (2) business days of identification.
6. In coordination with the Government PM and Subject Matter Expert (SME), fully resolve data issues: a) data patterns, b) trends, and c) understanding of database structure, entities and relationships. The Contractor shall develop queries to retrieve and analyze data and develop corrective scripts to fix data inconsistencies.
7. Contractor shall take corrective measures to lock/disable accounts as needed and directed.

**HELP DESK SUPPORT (FFP)**

The VA Enterprise Help Desk is a component of the overall Production Incident Escalation Communication process and includes a three-tier process. All user support calls are initially sent to the VA National Service Desk (NSD), which is responsible for Tier 1 support and uses ServiceNow to track all support calls. VA NSD will address any issues with the desktop, user access, network access, and printing.

The Contractor shall:

1. Develop the processes to provide the resources and tools that enable the capability of the escalation and resolution of issues.
2. Execute the resolution of help desk tickets.
   a. Provide support for an average volume of 15-30 data incidents across the PES product portfolio per week in Service Now.
   b. Provide support for escalation from Tier 2 to Tier 3 support.
   c. Provide support for the following tasks:
      1. Initial triage
      2. Data analysis
      3. Data query scripting and execution
      4. Data trends, data compromise, and data mismatch
      5. Ticket logging
      6. Advanced operational support
      7. Infrastructure and application layer troubleshooting
3. Provide a VA Tier 1 Help Desk communication plan to the existing VA Tier 1 Help Desk to identify methods by which the VA Help Desk is to communicate with the Contractor Help Desk.
   a. The Contractor shall establish dedicated, trained personnel to accept calls and manage repair requests requiring support.
   b. Any repair or maintenance request shall be traceable and auditable (a traceability/audit plan, when required, shall be submitted to and approved by the VA PM). The Contractor shall respond to issues escalated from VA Tier 1 within (24) hours.

   c. Develop an outline of steps for defect resolution. The Contractor shall ensure that all defect resolution steps are communicated to the Tier 1 support team.

4. Provide Tier 2 support of the production system by performing technical analysis and resolution of software defects impacting critical system functionality.
   a. If Tier 2 support is needed, the contractor shall respond within 1 hour of the start of the analysis to determine if there is a production outage. In the case of a production outage, a two (2) hour response time, and the team would be working in conjunction with affected incident/outage team(s).
   b. Execute initial triage of data issues as part of this task, including high level of expertise in determining trends in data that may be at risk of compromise.
   c. Perform analysis and resolution for fraud support.
   d. Data mismatch analysis, data inconsistency analysis and identification, slicing of data, determining root causes, and recommending solutions to secure data to complete an operational analysis of data and report findings to the product manager and COR.
   e. The Contractor shall provide an Incident and Defect metrics Report for each incident/ build/major issue using existing VA incident management and configuration management tools with details approved by the VA PM:
      1. Tracking of production defects
      2. Non-rework related issues
      3. Reliability and availability (%) trending
      4. Production data center processes
      5. Performance against defect
      6. Self-service evaluation of Contractor
      7. Backlog trends
      8. Issues and lessons from other help desks
      9. Defect tracking dashboards
      10. Process improvement recommendations
      11. Tickets reported by status and type
      12. Number of open, resolved, in progress, and closed tickets
      13. Days lost due to system failure and defects
      14. First call resolution metrics (wait time)
      15. Average time to resolve tickets
      16. Mean time between failure and escalations
5. Resolve all reported defects. The Contractor shall provide system and process support to ticket and defect resolution to comply with needs to inform all parties of the resolution of reported issues.
6. Leverage VA support system and tools to manage and report metrics for:
   a. Number of open, resolved, in progress, and closed tickets;
   b. Days lost due to system failure and defects;
   c. First call resolution metrics (wait time);
   d. Average time to resolve tickets;
   e. Mean time between failure and escalations;
   f. Monitoring of agent performance and statistics;

   g. A routing system that allows full-cycle traceability from initial Veteran request to resolution and escalation (as needed), to closure of issue. The routing system shall also be scalable to adapt to resolution of tickets

7. Support the logging of support tickets in VA approved tool(s).
8. The Contractor will coordinate with infrastructure and software teams to repair and resolve all activities related to maintenance.
9. Provide all Post Deployment Software Support tasks. Tasks include post deployment support, monitoring of sustainability of services, reliability of operations, escalation of issues, and resolution of defects found after a release.
10. Execute and deliver the timely installation of all security patches and virus scanning software in accordance with the VA approved schedule and security policies. Critical findings must be fixed within (30) days.
11. Validate, monitor, and operate/maintain continuity of operations for all services to include monitoring of dependent systems and databases.
12. Perform Defect Intake and Resolution.
    a. Determine support and test system requirements.
    b. Perform root cause analyses to replicate reported defects.
    c. Document processes to replicate reported defects in a VA approved tool.
    d. Perform regression testing after resolution of reported defects as required during each test cycle.
13. Perform Technical Analysis:
    a. Coordinate with the ISP to ensure protection against security vulnerabilities, intrusions and attacks and any other security risks.
    b. Ensure security of applications and associated data to prevent unapproved access.
    c. Develop Production Operation Manual (POM) and Information Systems Contingency Plan (ISCP). Execute failure analysis and disaster recovery processes documented in the POM/ISCP.
    d. Develop processes, scripts, and queries to monitor fraud and data inconsistencies. Perform root-cause analysis and develop scripts to prevent and correct data inconsistencies related to data fraud.
    e. Support Incidents and Major Incident Management (MIM) calls, coordinate, participate and provide updates per the Incident Management process:
        1. Provide root cause analysis and resolution
        2. Join MIM and provide operational support as required
        3. Support VA approved help desk requests and provide coordination and updates
        4. Support OIT PM VA requests for Incident and MIM updates
        5. Coordinate and track issues in Service Now, Jira and/or other report tracking system approved by the VA – update tracking system with resolution and mitigation strategies
        6. Analyze issues to understand patterns and develop mitigation to prevent and correct related issues.
14. Develop and deliver Help Desk reports at tempo coordinated with the PM to the COR/PM in an agreed upon format. Reports shall include, but are not limited to, the ability to sort and filter by incoming source, status, responsibility, open/resolved issues, etc. Other requests may include Recovery Time Objective (RTO) trends, SLA trends, time to close, backlog, number of tickets

open/closed by month, reliability, availability, un/planned down time, partner outages, maintenance and down times.

a. The Product Support Help Desk team lead shall deliver reports rolled up for two sprints, with a graphical representation useful for assessing trends and patterns. The following will be included:

**Table 1: Production System SLAs Severity Levels**

| Code | Customer Impact | Response to Customer | Resolution Goal |
|---|---|---|---|
| 1. Critical | Production System Unavailable | 0-15 minutes | 0-2 hours |
| 2. Major | Production System Delayed | 0-60 minutes | 2-4 hours |
| 3. Average | Production and Preproduction (Available – No Business Impact) | 0-4 hours | 4-8 hours |
| 4. Minor | New Service/Program Addition | 24 hours | 48 – 72 hours |

**Deliverables:**

A. Incident and Defect Report
B. Production Incident Escalation Communication Plan
C. Production Operation Manual (POM)
D. Information Systems Contingency Plan (ISCP).

### SPECIAL EVENT 24 X 7 SUPPORT (FFP)

For select events and occurrences within the specified product, the Contractor shall be required to provide services on a 24x7 basis. This includes production outages, as well as Major Incident Management (MIM) events involving the product and partner systems (approximately 1 per month which can take up to 48 hours to resolve), and interagency moratoriums declared by either VA or DoD.

### ON-CALL SUPPORT (FFP)

The Contractor shall provide after hours and weekend “On Call” support for network and external dependency tasks to support scheduled/coordinated and unscheduled activities and software releases. The Contractor shall create an automated alerting system, which varies in message type and communication based on the severity of the issue found, in order to provide outage alerts 24/7. Examples of the most common types of afterhours activities are below.

| Event | Frequency | Type of Support | Typical Duration | Longest Duration |
|---|---|---|---|---|
| Major Software Release | As often as every 2 weeks | Direct | 4 Hours | 10 Hours |
| Patch Release | As often as every 2 weeks | Direct | 2 Hours | 5 Hours |

| Event | Frequency | Type of Support | Typical Duration | Longest Duration |
|---|---|---|---|---|
| Minor Software Changes | As often as every 2 weeks | Indirect | 4 Hours | 10 Hours |
| External Consumer Updates | Every Month | Indirect | 5 Hours | 5 Hours |
| Closely Coupled System Maintenance | Once a quarter | Indirect | 8 Hours | 16 Hours |
| Break Fix | Once a Week | Direct | 4 Hours | 4 Hours |

Notifications are subject to triage processing that requires the Contractor to engage with other teams to validate the defect, propose a solution and implement the corrective actions.

For all major production support issues where the instance requires a source code change to mitigate the event, the Contractor shall provide the NSD lead, COR/Product Manager with an updated AAR. The AAR shall include the event description, analysis, determination of trigger, proposed and approved corrective actions, and follow up Root Cause Analysis.

For other major production events, the Contractor shall be required to update the RCA Report. The RCA shall include a summarization of the event, analysis, determination of trigger, and proposed corrective actions.

The Contractor shall provide notification to the COR/PM each time the status of a major production support issue or ticket changes within 24 hours.

The Contractor shall use, at a minimum, the following VA approved toolsets to perform operations and maintenance support tasks:

1. ServiceNow
2. JIRA
3. GitHub
4. MS Teams
5. MS SharePoint and the MS Office product suite
6. Other VA approved tools

For all other production support issues, the Contractor shall provide the following:

1. Update trouble tickets with the current status and a description of the solution or activities in progress needed to resolve the trouble ticket
2. Document and track production support issues that are considered application defects as Defect Work Items in JIRA or VA specified approved tool and map them to requirements for defect resolution. All defects should be prioritized and a timeframe for resolution will be approved by the VA COR/PM.

The COR/PM has adjudication authority for any changes in the priority and/or severity of a production support issue when the Contractor believes the priority and/or severity is incorrect.

The Contractor shall update the Incident, Problem, and Event Management Report, specified in section 5.1.10 above, which shall include the following:

1. Defect Backlog - Quantity closed, reassigned, revised, and those remaining open at completion of the phase-in transition to reestablish the Contractor's defect baseline for ongoing management.
2. Ticket Volume - Quantity received, closed, reassigned, newly opened (by the Contractor), or those introduced due to new releases, classified by severity. These metrics shall be referenced weekly (or more frequently as directed) and cumulatively, throughout the TO period.
3. Timeliness of trouble ticket resolution 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/PM's request.

### 5.2.2 PRODUCTION PERFORMANCE (FFP)

Production Performance tasks support of capacity planning, optimization, maintenance, and system monitoring. The Contractor shall comply with the approved VA process alignment Epic/User Story for capacity and scalability, in addition to other tasking and reporting as noted below:

1. Perform System Monitoring activities:
    a. Monitor uptime of all cloud infrastructure, hardware, servers, software, and services related to the Product.
    b. Develop dashboards and trend analyses to report spikes and issues that affect reliability, availability, and sustainability.
    c. Develop and deliver a productions Operations and Maintenance Plan (OMP) or equivalent.
    d. Develop and deliver reports, as requested by the OIT COR/PM, that show uptime and related partner issues that affect the availability of each Product.
2. Perform Capacity Management Plan activities:
   The Contractor shall perform analysis and provide associated services to ensure that IT capacity meets current and future business and VA requirements. The Contractor shall monitor availability and maintenance obligations to sustain IT service availability.
    a. Ensure planned capacity is sustained during operation and maintenance to support the maximum amount of resource demand for each Product and network infrastructure. Resource capacity shall be capable of supporting current maximum resource demand and planned for growth. Support monitoring during operations and maintenance to determine bottlenecks, root causes, and constraints, such as quality problems, code issues, service delays, network issues, and server issues. Monitoring during the release period) requires analysis of capacity monitoring alerts as they are generated.
    b. Compare trends and variances in monitored uptime to the baseline.
        1. Develop and deliver SLA capacity results report.

      2. SLA capacity results report shall be delivered monthly.
      3. SLA capacity results compare trends and average response times against the SLAs
      4. Capacity results monitor baseline and deviation from baseline.
      5. Capacity results report shall provide the above information for each service and service operation.
   c. Deliver a capacity management report comparing the actual capacity to both the established computational (CPU throughput, memory, storage, cloud resources, etc.) and network asset baseline as well as the projections in the SLAs, and highlight baseline discrepancies in the capacity performance of O&M. Identify the necessary computational and network assets above and beyond the current installed base at the time of the comparison that required to meet projected demand.
   d. Meet established service delivery requirements, SLAs, key performance indicators, and business goals. The Contractor is responsible for identifying the root cause of the performance degradation and effectively communicating with upstream and downstream dependent systems to ensure that resolution activities are completed.
   e. Perform corrective actions required to ensure that each Product is in compliance with established service levels and that design thresholds are not exceeded.

3. Perform Continuous Optimization Maintenance Activities:
   a. Manage notifications and alerts based on thresholds.
   b. Manage contingency planning and disaster recovery.
   c. Validate that data backups occur and can be restored with no data loss as directed by the OIT COR/PM.
   d. Validate the capacity baseline and the capacity management plan to develop and deliver a Continuous optimization plan & report that identifies the software and hardware resources required.
   e. Develop and deliver Product improvements based on the continuous optimization plan & report to support growth as outlined in the capacity management reports.
   f. On a quarterly basis, develop and deliver the continuous optimization plan & report that measures and details progress.
   g. Resolve service outages and issues and implement preventative actions to ensure that issues shall not reoccur.
   h. Analyze areas of the Product to determine capacity usage, document and fix issues.
   i. Establish the Capacity Baseline to support the development of features that will meet the capacity and performance requirements of the SLAs. Identify the resources required to meet the system SLAs by:
      1. monitoring the resource consumption trends of current services and their operations,
      2. modeling and projecting SLA consumption of resources,
      3. performance testing, developing and executing plans for resource consolidation, and stress testing of all tiers in each Product,
      4. identifying the resource gaps based on the existing resources (server CPU, memory, cache, and network bandwidth),
      5. identifying the necessary resources to meet the projects' needs stated in the SLAs,

6. preparing, submitting, and reviewing the SLA and Operational Level Agreement (OLA) with Infrastructure Support Provider.

j. Manage database optimization. The Contractor shall develop and deliver an analysis of the existing database schema and entities currently in usage and objects that shall be deprecated. After analysis is complete, apply industry best practices to optimize database for optimal performance.
k. Develop and deliver automated build and automated publishing capabilities to schedule jobs to support agile development and continuous integration for every sprint. Automated build tools shall be in compliance with the approved list from the TRM. This is to support automated build testing and automated testing of the build and publication process.
l. Define platform resource changes based on the continuous optimization plan quarterly and to support necessary growth.
m. Monitor thresholds, alarms, and resource consumption SLA compliance.
n. Develop and execute performance and load testing to support capacity planning.
o. Develop a baseline comparison of performance monitoring, including trends in usage and response times.
p. Support the development, updating, and monitoring of SLAs and ICDs with integration partners, and as part of each Product's architecture SDD, and manage dependencies, including measurement of up and down time and availability, baselines, and reliability of infrastructure, resources, and services.
q. Develop corrections to accommodate increased traffic to support the management of the Product environments.

To support management of the Production Environment, the Contractor shall validate and promote code and conduct testing in each Product's environments as follows:

1. Conduct Pre-Production (Pre-Prod) testing in a Pre-Prod environment inside the VA firewall. The Contractor shall coordinate with the appropriate teams prior to release to ensure compliance with VA release processes. Gate reviews are performed in the Pre-Prod environment prior to code promotion to production environments.
2. Promote code to the Production Environment after the successful completion of testing environments.
3. Manage the production environment to meet SLAs, escalate and resolve defects, and maintain a sustainable operating production environment.

**Deliverables:**

A. Capacity Management Plan & Report – Semi annual
B. SLA Capacity Results Report - Monthly
C. Quarterly Continuous Optimization Plan & Report
D. Service Level Agreements/Operational Level Agreement (SLA/OLA) Annual
E. Operations and Maintenance Plan (OMP) Annual

### 5.2.3 ENVIRONMENT MANAGEMENT (FFP)

The contractor shall ensure that appropriate lower environments are established for each product, and that these environments are operated and maintained per VA and Federal standards.
The Contractor shall:

1. Maintain Product environments, enable automated builds and build testing capabilities, include the validation of compiled code and check ins, fully automated and partially automated test scripts in the self-testing of builds.
1. Obtain VA approval to establish, configure and maintain each Product environments.
2. Provide VA with all relevant components, software elements, connectivity and configuration information necessary for VA to assess environment operations and maintenance (O&M).
3. Follow the standardized Code Promotion Process as defined in the CMP.
4. Configure product environment(s) and ensure that all development is performed within the VA approved environment. Any discrepancies shall be reported to the Project Manager within one (1) day of identification of discrepancies.
5. Support all operational aspects for code rollbacks.
6. Coordinate with the VA COR/PM to ensure that testers and support team members have access to detect and fix integration problems continuously throughout the project lifecycle.
7. Coordinate with the PM and Testing Team to perform integration and performance testing in a VA environment designated by the Change Control Board (CCB), or equivalent.
8. Submit software build and supporting documentation in accordance with VA approved processes.
9. Ensure the availability, configuration, and maintenance of the product environments are consistent with test and release planning as well as mandated Continuous Readiness in Information Security Program (CRISP) maintenance.
10. The team shall document a deployment, installation, roll back, and back out guide. Coordinate with the VA COR/PM to identify and test changes needed in all product environments.
11. Coordinate with the VA COR/PM and the Release Manager prior to each release to ensure artifacts comply with VA release processes.

### ENVIRONMENT MONITORING AND ANALYTICS (FFP)

The Contractor shall provide operations monitoring and analysis for each product's related services in all environments. The Contractor shall:

1. Monitor services and applications to detect service delays, network issues, and server issues.
2. Monitor product system components to sustain IT service-availability and support planning and analysis determine bottlenecks, root causes, and constraints, such as quality problems, code issues, for system performance and capacity improvements.
3. Monitor uptime for all hardware, servers, software, and services related to the product.
4. Maintain and develop dashboards and trend analyses to report spikes and issues that affect reliability, availability, and sustainability).

### LOGGING AND AUDITING (FFP)

The Contractor shall:

1. Monitor logs, run queries for data consistency, data mismatch, and identify risks related to data compromise. The Contractor shall complete auditing tasks, deliver analysis and reports to the COR/PM and ISSO.
2. Provide support for transactional data analytics with tools implemented at the ISP. The tools listed and used for logging and auditing shall be in compliance with the VA TRM.
3. Provide automated reports from the activity and audit logging tools.

## ENVIRONMENT MANAGEMENT | CODE PROMOTION (FFP)

The Contractor shall:

1. Develop code in an environment that is configured by the Contractor and hosted by the VA. The code and build shall be tested across the lower environments. The Contractor shall coordinate with stakeholders/partners to test in the lower environments.
2. Conduct performance testing to stress and load the system with the intent of certifying the code for capacity, latency, and throughput of transactions. Testing shall also be used to evaluate the performance of the infrastructure as new features are deployed and shall be tested for every release.
3. Conduct Quality Assurance (QA) testing. All phases of testing, defect tracking and resolution shall occur within the lower product environment.
4. Promote candidate builds to the production environment after the successful completion of testing in all lower-level environments and upon approval by Product PM. Contractor shall provide release documentation and release notes.
5. Validate with the ISP prior to release to ensure compliance with VA release processes.
6. Update VA Dashboard, or VA approved dashboard, with all above information.

**Deliverables:**

A. Release Documentation and Release Notes
B. Test Plans
C. Test Results
D. Monthly metric reports on for Environment Monitoring, auditing, and system uptime. Current requirement is VA PARS report card.
E. eMASS reports on security

## ENVIRONMENT CONFIGURATION SUPPORT (FFP)

The Contractor shall:

1. Configure Product component and applications, maintain, develop, integrate, and support testing in all environments and work with the VA COR/PM to coordinate installs into ISP managed environments.
2. Lead the deployment of configuration items.
3. Perform/provide product / system configuration changes shall be automated and scripted so that the probability of human errors is reduced, configuration changes are approved and tested before they are introduced to production environments.
4. Manage all environments, typical environments are Sandbox, Development, Quality Assurance, Integration/Staging, Preproduction, Production, and/or build.

5. Patch systems based on the VA COR/PM approval of the ISP proposed maintenance and patching schedule.
6. Perform software installation and configuration for VA provided support in development and test environments and work with the VA COR/PM to coordinate installs into ISP managed environments.
7. Perform database maintenance in all environments for applications and users. The Contractor shall maintain the database, ensure operating efficiency and processing (cleaning up deleted records, re-indexing, creating new indexes and views, backing up, and partitioning).
8. Support configuration for data exchange with business partners, customers, and other entities (ex., file transfer protocol (FTP), Electronic Data Interchange (EDI), e-commerce connections for ordering, copying data between servers).
9. Provide port management (e.g., the opening and closing ports on the firewall to allow the network to communicate with outside servers).
10. Provide server management for applications and infrastructure.
11. Support all operational requirements for code rollbacks.
12. Develop the information required to support infrastructure configuration for internal and external IT communications, including router, hubs, firewalls, DNS servers, file servers and load balancers.
13. Support the configuration of ticket information and support workflow (new, open, assigned, resolved, closed, or other workflow phases) as required by the Project Manager.
14. Post and track artifacts into the document repository or VA specified tool.
15. Coordinate with the PM Team to ensure accurate updates of architectural and system design documents and diagram for each Product environment (including data flows, software versions, components, and services) are provided with each environment change.

## ASSESSMENT AND AUTHORIZATION (FFP)

The Contractor shall achieve and maintain full Assessment and Authorization certification, in compliance with VA Handbook 6500.

The Contractor shall:

1. Perform all O&M activities related to acquiring and maintaining ATO within the VA network or cloud environment for each applicable system.
2. Participate in Security Control Assessment (SCA) and remediate findings.
3. Ensure all security assessments are completed in eMASS or a VA mandated tool.
4. Respond to VA enterprise vulnerability scanning and prioritize corrective actions to mitigate identified weaknesses and vulnerabilities.
5. Mitigate vulnerabilities and address controls.
6. Perform continuous monitoring per VA's Continuous Readiness in Information Security Program (CRISP).
7. Within the product's ATO Boundary, using NIST Special Publications as a guide, secure logical and physical infrastructures for Information Systems (IS) environments including, but not

limited to security plans, risk assessments, access controls, directory services, security management, compliance monitoring, vulnerability scanning systems, firewalls, intrusion prevention, intrusion detection, anti-virus tools, privacy impact assessment, and PII and other data protection policies.

8. Identify, mitigate and resolve information assurance (IA) issues and concerns, including existing and newly identified information system vulnerabilities associated with application systems.
9. Develop and perform Standard Operating Procedures (SOP) management and tasking as defined in A&A documentation.

## AUTHORITY TO OPERATE (FFP)

In support of the Information System Owner (ISO) and Information System Security Officer (ISSO) the Contractor shall provide information assurance resources to manage the VA ATO process. Examples are to create and manage applicable documentation, coordinate with partner applications, and provide consistency with VA ATO requirements for certification. Ensure the supported applications/systems meet VA information security policies and standards. Facilitate the successful completion, and ongoing management, of the Assessment & Authorization (A&A) process and obtain/maintain the application's ATO.

The Contractor shall:

1. Support VA ISO, ISSO, and the Office of Cyber Security Control Assessment team as detailed in VA Directive and Handbook 6500 Information Security Program and Accreditation of VA Information Systems.
2. Conduct cybersecurity software code quality testing and validation of all software code and provide certified scan reports validating the required code quality.
3. Conduct and participate in vulnerability scans and tests as detailed in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 5 Recommended Security Controls for Federal Information Systems and Organizations, if/when requested by the COR/PM.
4. Security scanning shall be performed by multiple methods and is performed multiple times throughout the course of a project with methods such as infiltration testing, code analysis tools (e.g.,CodeQL, Fortify), etc.
5. Remediate all vulnerabilities identified in government scans or quality checks or reviews (Secure Code Review/Quality Code Review require remediation of all findings) for approval by appropriate VA governing group.
6. Provide vulnerability scanning reports and assessments as detailed in NIST SP 800-30 Rev 1 Guide for Conducting Risk Assessments.
7. Support each product by identifying, documenting, reviewing, and maintaining the A&A artifacts to support an ATO request in accordance with VA policy and Federal Law and guidelines, as detailed in NIST SP 800-37 Rev 2 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Additionally, the

Contractor shall update any aspect (e.g. documentation, code, etc.) of the effort based on comments from the A&A review process conducted.

The A&A artifacts may include, depending on hosting location (on prem or Cloud), but are not limited to the following:

1. System Security Plan (SSP)
2. Security Configuration Plan (SCP)
3. Information System Contingency Plan (ISCP) (coordinate with Office of Business Continuity)
4. Incident Response Plan (IRP)
5. Privacy Impact Assessment (PIA) (coordinate with Office of Privacy)
6. Risk Assessment (RA) (coordinate with Office of Risk Management and Incident Reporting)
7. Security Configuration Checklist (SCC)
8. System Interconnection Agreements (Memorandum of Understanding [MOU], and Interconnection)
9. Interconnection Security Agreement (ISA) as necessary
10. Standard Operating Procedures (SOP)
11. Signatory Authority
12. Manage governance tool (currently eMASS).

The Contractor shall also provide continued security Plan of Action and Milestones (POAM) support. Any VA directed vulnerability scans, remediation and reports must be completed prior to the conduct of the VA acceptance testing.

### 5.2.4 USER GUIDE UPDATES (FFP)

The Contractor shall create/update any documentation that addresses procedural information for the users of products including GUIs on daily operational use of the software, knowledge articles (i.e.,text or video) and help tips. The updates shall include changes resulting from new development, sustainment or user feedback. Acronym/jargon is kept to a minimum or explained thoroughly. The document reflects the contents of the most recently deployed build and is updated to include the changes for each build.

### 5.2.5 SOLUTION TRAINING (FFP)

The Contractor shall provide training for products with end users for VA staff in the utilization and O&M of solution applications, components and services completion for each production development cycle for the duration of this TO.

The Contractor shall provide Virtual training to the VA as specified below.

1. Perform collaborative sessions with the VA Training POCs throughout the process of developing training materials to ensure that they meet the needs of the training team.
2. Provide a walk-through of all training materials prior to the start of training sessions to the end users.
3. Perform hands-on training with VA Help Desk personnel (not to exceed a total of 15 users) prior to the delivery of the solution for production. Provide minutes of training sessions to include a list of attendees, and time attended.
4. Perform hands-on training with System Administrators/Operations staff (not to exceed a total of 25 users) prior to the delivery of the solution for production. Provide minutes of training session to include a list of attendees and time attended.
5. Develop, update and maintain training materials, user guides, developer guides and online help artifacts to be consistent with system enhancements. Additionally, all training materials shall remain current and shall be updated to reflect the most current information.

**Deliverables:**

A. End-User Training Package and minutes

## 5.3 CDW SUPPORT SERVICES

### 5.3.1 CDW ADMINISTRATION AND SUPPORT SERVICES (T&M)

The Contractor shall perform database administration tasks for the CDW environment. CDW provides national authoritative health and enterprise data and analytic tools at scale to 23,000+ developer/analysts from 7,500+ workgroups. These workgroups create downstream data products that get consumed by 100,000+ content customers including Veterans, Congress, Inter-agency partners, VA Senior Leaders, Health Research, and National/Field Healthcare Operations. CDW Administration and support services cover a wide spectrum of disciplines. These areas of coverage are outlined below.

Systems Administration (SA)

1. Servers: Building, managing, maintaining, and monitoring CDW/VINCI server systems.
2. Data Center: Planning and installation of all on prem systems and coordination for data center resources.
3. Infrastructure: Integration of the Windows, LINUX, network and storage teams systems into a single infrastructure.
4. Network / Storage: Managing the network and storage systems for CDW and shared infrastructure with VINCI and DMM.
5. Backups: Responsible for the physical backups of CDW systems and data.
6. ATO: Responsible for ATO and overall security implementation; Security Technical Implementation Guidelines (STIGs), Group Policy Updates(GPO), vulnerability remediation, security scans and reports.

### Data Integration (DI)

1. CDW On-Premises: Responsible for development and operations for all CDW Vista, Millennium and National data projects.
2. CDW Next Generation: Responsible for development and operations of the CDW Next Generation data lake.
3. On-Call Responsibilities: Responsible for all daily ETL processes, along with research and support of any customer data quality issues.
4. Data Distribution: Responsible for development of new functionality and maintenance of existing code for the Data Distribution System (DDS).
5. Performance Troubleshooting: Periodic work to ensure the most efficient processing of packages, tables, and other processes.

### Data Source Extraction (DSE)

1. System Administration: Maintain the configuration of CDW shadow-servers (Linux), Maintain Data Filers (Windows), apply updates, firmware updates.
2. Data Check Management: Develop enhancements to the Data Check methods used to compare site databases with shadow-copies of site databases.
3. Data Quality: Address any Data Quality issues between the VistA sites and the CDW shadow-copies of the sites.
4. Other Technical Tasks: Software tool management, system monitoring, site migrations and upgrades, eHRM/Cerner Support, VX-130 Support, and CDW initiative coordination.

### Data Management (DM)

1. Database Backup/Restore: Provides backup and restore operations on databases across CDW.
2. Database Security: Ensures consistency of database permissions across CDW.
3. Deployment of CDW Objects: Supporting CDW Architecture team implementing tables, indexes, views, and writing SQL layer of BaseCamp.
4. SQL Server Management: Installation, Upgrades, and Maintenance and general support for 70+ SQL instances.
5. Performance Monitoring and Troubleshooting: SQL Server analysis and resolutions; monitoring enclave performance; query termination policies across CDW enclaves.
6. CDW Raw Extracts: Operate the CDW-Raw Extractor using Oracle Forms, J2EE/J2SE, and WebLogic on specified schedule.
7. DBA Metrics: Requirements, collectors, reports.
8. Provide DBA expertise for critical projects such as CDW Raw Extractor, GoldenGate, SQL52, PERC Enclave-SQL20 in memory tables, outage data to DBA Metrics, DBATools.IO and query termination.

### Data Architecture (DA)

1. Data Modeling: Gather and translate functional requirements to technical requirements for designing/creating staging and loading table data models.
2. Metadata: Ownership/oversight/maintenance/socialization.

3. Domain Release Management: Manage CDW Object Deployment System (CODS), create ER Diagrams and Release Documents.
4. Data Syndication Support: CDWWork2 build new tables and optimize existing tables; CDWWork3 support.
5. Development: Process Automation/Optimization including Metadata Editor application maintenance.

### Customer Resource Management (CRM) Tool Sustainment and Enhancement

1. BaseCamp Development: AGILE development of the D&A Customer Resource Management tool integrating cloud and on-premises.
2. Sustain and Improvement: Maintain operational usage for over 7,000 operational and research workgroups in current use while adding functionality.
3. Automation: Transform bespoke/manual processes to rule-based automation for resource provisioning and data sharing.
4. Stakeholder Engagement: Basecamp uses a robust User Acceptance Testing (UAT) to ensure the release tempo meets customer requirements with minimal downtime.
5. Security Tracking: Basecamp enforces data categorization rules when sharing along with visibility on high-value data.

### Enterprise Geospatial (EG)

1. GIS Services: Provide GIS support services, training, and development to CDW customers and other key stakeholders.
2. Geocoding: Converting Street address into Latitudinal/Longitudinal coordinates.
3. Common Special Data: Provide common non-PHI/PII data to users.
4. GIS Infrastructure and Software: Provide and support desktop GIS software and Enterprise GIS infrastructure.
5. Geospatial Database Management: Provide DBA support and expertise for managing spatial data within SQL Server.

### Enterprise Tools (ET)

1. Power BI Cloud Services: Administration, resource provisioning, customer support, customer training, policy management and upgrade/feature integration.
2. Power BI Report Server: System admin/monitoring, communications and documentation, content development, modernization/automation, and customer support
3. Pyramid Analytics: Pyramid system architecture, monitoring, and functionality, training, special projects, customer support and communications and application upgrades and software improvements.
4. SQL Server Analysis Services (SSAS): SSAS server management & cube management, VM coordination, on-call responsibilities, developer support, BISL team support.

### Enterprise Initiatives (EI)

1. Access to Care (AtC): Power BI reporting: site management, API management, site security, data refreshes through Azure Data Factory and automation. project management.

2. National Surveillance Tools (NST): maintain and enhance data mart, monitor and troubleshoot ETL and data profiling jobs.
3. Office of Mental Health and Suicide Prevention (OMHSP)/PERC and Electronic Quality Measures (EQM)): Maintain and enhance databases/enclave, maintain and enhance web applications, support and update curated data objects, perform data integration from desperate sources, and monitor and troubleshoot data distribution jobs.

## 5.4 VINCI SYSTEM ADMINISTRATION SERVICES

### 5.4.1 VINCI STORAGE AND SYSTEM ADMINISTRATION (FFP)

The Contractor shall:

1. Design configurations, install, administer, and tune 6 Brocade Fiber Channel Switches, consisting of (2) X6 Director, (2) X7 Director, and (2) 6520s. Total port count of 1440.
2. Design configurations, install, administer, and tune data storage devices (disk). This ~~c~~ consists of Seven (7) HPE Storage Arrays, one (1) Netapp A300 Array, twelve (12) HP Virtual Library System (VLS) Arrays, one, one (1) Backblaze Cluster, one (1) Windows Storage Spaces Cluster, and 16 Pure Storage devices. The total disk storage capacity for VINCI is approximately twelve (12) PetaBytes
3. The Contractor shall provide and maintain a report on the storage capacity on all Storage Arrays and the percentage of space utilized as part of Weekly Status Report.
4. Administer Storage Support Consoles and Software including, HPE Infosight, HPE SSMC, HP 3PAR Management Console, HP 3PAR-InformOS Command Level Interface (CLI) , HP 3PAR Service Processor Onsite Customer Care (SPOCC) , Netapp OnTap, Netapp OnCommand, Netappp Unified Manager, Pure Storage PureOne, Pure Storage Dashboard.
5. Actively monitor disk storage capacity and switches, providing utilization and performance graphs and statistics using monitoring tools. The tools consist of HPE SSMC, HPE Infosight, Solarwinds, Broadcom SAN NAV, and Netapp Unified Manager.
6. Provide integration services for new disk storage into the VINCI environment.
7. Provide technical refresh data migration services from existing disk data storage devices to newly acquired disk storage devices.
8. Coordinate multiple vendor support for complex problem resolution of hardware errors, software issues and firmware upgrades
9. Perform Backup Operations including hierarchical storage management, Using Commvault and SQL22 Backup Manager to Pure Storage Flashblade.
10. Configure and manage AZURE archive backups.
11. Provide System Technical Guide on Configurations and Topology, including Topology Diagrams for all hardware, Build Guide for each system, and Configuration Guide for each system; Provide Mapping of Storage Documentation to each initiative, Lifecycle Migration Plan for all equipment and provide ATO documentation as necessary.

**Deliverable**:

A. Weekly Status Report
B. Technical Guide on Configurations and Topology

C. Mapping of Storage Documentation
D. Lifecycle Migration Plan

### 5.4.2 BACKUP ADMINISTRATION (FFP)

The Contractor shall:

1. Schedule and maintain backup jobs for all systems (Linux and Windows) (backup varies from system to system; generally, data consists of two (2) PetaBytes of information dispersed over 190 physical systems that are primarily Windows. Approximately 15 percent of the systems are Linux) using Microsoft Data Protector Manager and HP Data Protector, Commvault or similar software.
2. Administer backup servers (Linux and Windows) for Microsoft Data Protector Manager and HP Data Protector or similar software.
3. Troubleshoot and repair failed backups and bottlenecks.
4. Upgrade backup software approximately twice per year.
5. Perform hardware upgrades on backup environment: Servers, Virtual Tape Library System (VTLS), tape drives and tapes approximately twice per year.
6. Generate daily and weekly reports from each backup application for backup success/failures, which shall be delivered as part of the Weekly Status Report.
7. Maintain backup devices for each hardware platform Enterprise Storage Library (ES) and VTLS.
8. Conduct Backup software installation/upgrade/patching.
9. Conduct Backups load balancing and optimizations.
10. Administer HP Data Protector, Commvault or similar devices, policies, backup specifications, templates, and global configuration settings.
11. Monitor and adjust to keep optimal system performance and identify any input/output (I/O) bottlenecks during backup.
12. Create and maintain custom HP Data Protector Report as part of the Weekly Status Report.
13. Create and maintain Pre/Post backup scripts (custom scripts ran before and after backup job) as part of the Weekly Status Report. Any failed backup issues shall be reported weekly by telephone or email to VINCI technical PM.
14. Integrate and administer HP Command View Tape Library.
15. Administer Commvault or other backup software being used in the VINCI environment and associated devices.
16. Perform data restorations approximately twice per quarter as directed by VINCI technical PM.
17. Perform Tape life cycle management and tracking.
18. Report any system issues and document any system additions or modifications as part of the Weekly Status Report.
19. Provide Build guides, Configuration guide, Backup Management Plan, Lifecycle migration plan for all equipment and ATO documentation updated as necessary.

### 5.4.3 LINUX ADMINISTRATION (FFP)

The Contractor shall:

1. Administer Linux SAS 9.X Grid with Linux Clustering.
2. Administer Hadoop 3.X Cluster (Hortonworks implementation).
3. Administer and maintain Red Hat Enterprise Linux (RHEL 7 and 8) and CentOS versions 6.x and 7.x.
4. Support Linux authentication with Centrify Software to Windows Domain Controller both musts support PIV card authentication.
5. Configure and maintain CDW Cache shadow servers.
6. Harden servers per VA STIG.
7. Perform operating system upgrades and patching approximately twice per quarter.
8. Perform monthly security patching and vulnerability remediation.
9. Reconfigure system architecture (for example clustering, adding additional storage, configuring system setting) for new solutions.
10. Work with application administrators to examine and analyze an application for when it is, e.g. slow, erroneous or non-functional, to ensure a positive customer experience.
11. Monitor server logs and proactively address issues.
12. Respond to and remediate outages – this may occur after business hours.
13. Maintain a consistent configuration baseline.
14. Build Windows and Linux systems with from bare metal, both virtual and physical.
15. Implement Linux/Windows interoperability solutions.
16. Identify opportunities for system and environment improvement and report weekly by telephone or email to VINCI technical PM.
17. Minimize impact of security scans and record in system log.
18. Sustainment and upgrades to security access mechanisms such as PIV and Active directory
19. Track historical server performance metrics using existing log file or database.
20. Identify trends to proactively address potential performance bottlenecks.
21. Explore system information to support potential solution.
22. Patch all systems to minimize security vulnerabilities as pertain to the ATO.
23. Verify weekly backups by checking the backup application log.
24. Provide report on any system issues and document any system addition or modifications as part of the Weekly Status Report.
25. Provide configuration guides for each system, ATO documentation updated as necessary, Documentation of bugs/fixes and user interactions and help desk ticket tracking and closure. This guide must be update upon addition or modification of any new or existing systems.

Deliverable:

A. Weekly Status Report

### 5.4.4 WINDOWS ADMINISTRATION (FFP)

The Contractor shall:

1. Install, configure and maintain approved Operating system (OS) versions which can include Windows 2019, ~~2016, 2012 R2, 2016~~ including OS patching, drivers and hardware firmware.
2. Harden servers per VA STIG guidelines
3. Perform operating system upgrades and patching weekly or as needed.
4. Adjust or migrate physical and virtual machines to the cloud.
5. Perform monthly security patching and vulnerability remediation.
6. Administer Microsoft HYPER-V clusters and Virtual Machine Manager
7. Perform Physical and Virtual server builds weekly.
8. Conduct System optimization and updating.
9. Conduct General Windows System troubleshooting.
10. Conduct Server performance bottleneck troubleshooting.
11. Maintain or create group policies/ local policies required by AITC/VA security entities.
12. Assist with troubleshooting RDP issues from clients.
13. Maintain Microsoft Forefront Threat Management Gateway (TMG) servers as the firewall for VINCI by creating/removing/modifying security policies monthly or as needed.
14. Rack and stack procured hardware (different contract – approximately $1.5M hardware and software per year) including running network and fiber cables.
15. Maintain Applications (commercially available and VA developed applications) through Microsoft terminal services application deployment services.
16. Administer System Center Operations Manager - upgrade, configuration & maintenance.
17. Patch all VINCI systems to minimize security vulnerabilities and stay in ATO compliance.
18. Verify weekly backups by checking the backup application log.
19. Report on any system issues and document any system addition or modifications as part of the Weekly Status Report.
20. Provide Configuration Guides for each system, updated ATO documentation as necessary, Bug/Fix Documentation and a user interaction and Help desk Ticket tracking (Section 5.2.1) or email request and closure.

### 5.4.5 SYSTEM MAINTENANCE SUPPORT (FFP)

The Contractor shall provide system maintenance and support to all components in the VINCI environment. The VINCI system has many components including but not limited to:

SAN

- HPE- Primera 670 (3), 20800 (1), 8400 (2, to be decom), 7400 (1, to be decom)
- Broadcom X6 and X7 director switches (4 total that are supported)
- Tegile- T4200 (1, to be decom)
- PureStorage- X50 (3), X90 (1), XL130 (4), C60 (5), Flashblade
- Netapp AFF300 cluster (2 heads)

Ethernet Network

- Cisco Nexus 9504's and 93180's
- Cisco Catalyst 9300's
- Mellanox SN700's SN2100's SH2200 and SX1018's

- F5 I5800’s load balancers
- Palo Alto 5260 firewalls

Servers

- HP ProLiant DL580 Gen9 & 10 servers
- HP ProLiant DL 560 Gen9 servers
- HP ProLiant DL 380 Gen9 servers
- HPE Flex 280 servers
- HPE Synergy enclosures (Prod)
- SY480 and SY660 Gen10
- HP ProLiant C7000 enclosures (Dev/Test)
- BL460c and BL660C Gen9 blade servers
- DL380 Gen10 GPU Systems
- DL360 Gen10 GPU Systems
- HPE StoreEver G3 Enterprise Tape Library (to be decommissioned)
- Spectra Logic (SpectraStack) Enterprise Tape Library

Storage/Backups:

- NetApp FAS8040
- Tegile T4200 hybrid array
- HPE 3PAR 20800
- Pure Storage m20R2 all-flash array
- Windows Storage Spaces (DataON DNS-2670D)

Ethernet Network

- Cisco 2232 and other Switches

Fiber Channel

- HPE SN8600B director switches and blades
- Cisco Nexus 2232 fabric extender

Servers

- HP ProLiant BL460c and BL660C Gen9 blade servers
- HP ProLiant DL580 Gen9 servers
- HP ProLiant BLc7000 enclosures
- HPE 280 Flex servers
- DL380 GPU Systems

## 5.5 SOFTWARE DEVELOPMENT (FFP&T&M)

The Contractor shall perform software development to include new features with the goal of increasing efficiency and reliability on a continuous basis. This Optional Task may be applied to any of the products.

In addition to 5.5.X subparagraphs requirements below, the following O&M subparagraphs apply to development activities:

| | |
|---|---|
| 5.2 | Operations & Maintenance |
| 5.2.1 | Production Support |
| 5.2.2 | Production Operations Support |
| 5.2.3 | Continuity of Operations and Disaster Recovery |
| 5.2.4 | Continuous Integration |
| 5.2.5 | Systems Administration |
| 5.2.6 | Help Desk Support |
| 5.2.7 | Special Event 24 x 7 Support |
| 5.2.8 | On-Call Support |
| 5.2.9 | O&M Warranty Support |
| 5.2.10 | Production Performance |
| 5.2.11 | Environment Management |
| 5.2.12 | Environment Monitoring and Analytics |
| 5.2.13 | Logging and Auditing |
| 5.2.14 | Environment Management/Code Promotion |
| 5.2.15 | Environment Configuration Support |
| 5.2.16 | Systems Security Support |
| 5.2.17 | Assessment and Authorization |
| 5.2.18 | Authority to Operate |
| 5.2.19 | User Guide Updates |
| 5.2.20 | Solution Training |
| 5.2.21 | Operating System Patching |
| 5.2.22 | Third-Party Software Patching |
| 5.2.23 | Network Infrastructure Configuration and Device Patching |

The Contractor shall develop new features under this TO as per the subparagraphs below.

### 5.5.1 RESOURCE PLANNING Optional Task (FFP)

The Contractor shall:

1. Provide a Resourcing Plan, for review and approval by the VA, with expert resources consistent with the Scaled Agile Framework (SAFe) and DevOps practices. Resource planning shall include providing scrum teams (as described in Section 4.6.1) to follow the Scrum Agile methodology. The 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.
2. Provide necessary development management resources such as a Scrum Master and Release Train Engineer and Test Lead amongst critical roles to support each SAFe release cycle, to include defect management support following the release of all software into production.

**Deliverables:**

A. Resourcing Plan

### 5.5.2 AGILE/SAFe REQUIREMENTS ELABORATION (FFP)

The Contractor shall perform Agile project management and planning. Agile processes are intended to produce high quality results in a cost effective, timely, and highly collaborative manner, which requires communication among all participants. The Contractor shall execute all planning and design tasking to develop a service that operates in either the current as-is environment or a to-be architecture and environment advised by the Project Manager given at the start of each build.

The Contractor shall complete an initial backlog grooming session with the VA team to properly understand and elaborate business Agile requirements.

Also, the Contractor shall:

1. Ensure all epics, including alignment epics are included and executed as appropriate within the overall agile backlog grooming effort.
2. 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 and with approval by the VA COR/PM.
3. Establish initial unit of measurement (e.g., Story Points) as the estimated relative complexity of user stories.
4. Facilitate any stakeholder briefings, meetings and/or elicitation sessions.
5. Execute requirements reviews with stakeholders and record results of reviews using Jira or other VA approved tool, updating requirements data as a result of the reviews.
6. Identify and set up any environment access that is needed 30 days prior to development start.
7. All Epics, stakeholder needs, visualizations, stories, and other sources of requirements information for functional and non-functional requirements are entered and maintained in Jira or other VA approved tool. 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.
8. Identify all partner dependencies required to meet requirements. Dependencies should be included in project schedules and communicated to the necessary parties.

**Deliverables:**

A. Initial and groomed backlog of requirements

### 5.5.3 BUILD AND DEVELOPMENT (FFP)

The Contractor shall continuously support the iterative build and development methodology to complete all epics and user stories identified in the backlog leveraging Software Engineering best practices. A build may consist of planning, development, testing and release activities. The number of sprint teams, duration, scope and set of deliverables associated with each build will be agreed upon by the VA COR/PM prior to build start. The Contractor shall initiate Sprint Planning at the beginning of each sprint included in the build. The Contractor shall maintain the product backlog, continuously, for each build, in every release and throughout the life of the PoP within Jira or other VA approved tool. All activity scheduled in each build and backlogs will be captured and have status showing all work items, changes, impediments, and retrospectives. The Contractor shall document all activity executed in each sprint and updates to the backlog in Jira or other VA approved tool including all project artifacts such as work items, changes, risks, issues, impediments, and retrospectives. All data and artifacts in Jira, GitHub or other VA approved tool(s) shall be fully linked to requirements data and test data to maintain a Requirements Traceability Matrix (RTM). All project artifacts and source code will be under change and configuration management as specified by the COR/PM using Jira, GitHub or other approved VA tool(s).

### SOLUTION ARCHITECTURE PLANNING AND EXECUTION (FFP)

The Contractor shall create solution architectures that include the business, systems, application, and data architectures for the new features and capabilities using an architecture framework, and TRM approved solutions for each product, approved by the COR/PM. The collection of these documents will be referred to as the Solution Architecture Package. These documents shall be updated utilizing VA approved templates and Jira, Confluence or other VA approved tool when appropriate, and approved by the VA COR/ PM in each subsequent sprint. Each subsequent update shall include versioning, which specifies the updates made to the document for review and approval by the VA COR/ PM. The Contractor shall also outline any initial gaps, questions or challenges that may hinder progress in future builds or sprints.

The Contractor shall:

1. Be responsible for setting up all necessary environments. These environments shall be used to complete all development and testing activities.
2. Create the necessary test data that will be used to verify that the development work produces the expected result.
3. The Contractor shall use VA approved tools to engineer, develop and deliver automated build and automated publishing capabilities to schedule jobs and support continuous integration for every sprint. The code shall be demonstrated to the Government for approval by the COR/PM to be promoted to another environment without issue by evidence of the status of tests and results in Jira or other VA approved tool.
4. The Contractor shall use VA approved tools to perform Code Analysis to ensure security and code quality issues are addressed within a sprint.
5. The Contractor shall address all gaps, questions, and challenges the potentially hinder progress.

**Deliverable:**

A. Requirement Traceability Matrix (RTM)
B. Solution Architecture Package

**DATA ARCHITECTURE PLANNING SUPPORT (FFP)**

For each new data domain, the Contractor shall:

1. Produce a set of data models that address the domain after analysis has been completed

- Conceptual Data Model (CDM): Deliver a high-level representation of the organization's data entities, their relationships, and attributes.
- Logical Data Model (LDM): Develop a detailed representation of the data structure, including data types, constraints, and normalization rules.
- Physical Data Model (PDM): Create a model that maps the logical data model to the specific database or data storage system.

2. Assist with modeling, data architecture, and meta-data for the common customer information domains.

3. Support development of reports to VA Data Governance Council and support OI&T efforts to implement data governance practices across supported systems and products.

The Contractor shall:

1. Define and model the Customer Record for enterprise customer information.
2. Assist with defining extraction, transformation and load (ETL) processes from the various heterogeneous sources systems across the VA Lines of Business.
3. Design and model enhancements to the Enterprise Data Quality / Master Data solution
4. Maintain the Common data model, including data dictionary
5. Support and maintain Enterprise data quality patterns for Veteran customer information.
6. Support and maintain Enterprise data policy rules for Veteran customer information), as part of the Solution Architecture Package, provide Enterprise Customer Data Models (conceptual and logical).
7. Determine how organizational policies and rules will be applied to common veteran data (e.g.,contact information, demographic data).
8. Collaborate with product owners to document and provide Business Interface Objects (BIOs), as part of the Solution Architecture Package, that define the business rules and processes for each data domain.
9. Collaborate with product owners to document and provide Feature Files, as part of the Solution Architecture Package (Use Case) to describe the specific functions of the software.

**BUILD PLANNING (FFP)**

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance. The Contractor shall develop and deliver a Build Plan in collaboration with the project team(s) prior to beginning the build for each Product. The Build Plan is the scope of work which will be completed in the agreed upon build timeframe. Each build shall end with a minimum of one new release or push to production. The PM shall define the duration period for each build/increment and shall be made up of individual sprints. 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 build plan. Planning for future builds will occur during the execution of current build.

For products with a large backlog, Program Increment Planning (PI Planning) events are held. For these products, the contractor will lead and help manage the PI Planning event and deliverables. For products that require PI Planning events, the deliverables and items listed below will be elaborated.

The Contractor shall:

1. Facilitate review, elaboration, and prioritization of the backlog.
2. Facilitate selection of prioritized items from the product backlog to be included in the next build/increment with approval of VA COR/PM and incorporate those items into a Build Plan for posting to the VA approved tool.
3. Conduct an Initial Design Review with stakeholders to ensure the design is technically and fiscally able to be completed during the build/increment.
4. Coordinate and support Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU) and Service Level Agreements (SLAs) for partner dependencies that specifically highlight the commitment of partners to the associated release. The ISA specifies the technical and security requirement of the interconnection, and the MOU defines the responsibilities of the participating organizations.
5. Develop estimated level of work (Story Points), potential risks, dependencies, and obtain government approval for each build Candidate package and build number recommendations.
6. Update the SDD that describes developmental changes being performed on services that are being modernized or enhanced. The SDD shall include detailed descriptions and configuration settings for each service in the SDD and serves as the master product description for each service. SDD content is service specific and similar in function to technical stories.
7. Obtain approval from the PM to develop or change services. Once approved, changes will be formally incorporated into the SDD.
8. The Contractor shall add any new or missing service-related technical stories into the build backlog for implementation.
9. In the event the Contractor identifies discrepancies (e.g., errors/omissions) of epics, user stories, and/or technical stories during build planning, they shall notify the Project Manager within two days of the discrepancy.

10. Use the VA approved tool to structure, store and maintain build plans, and ensure that the status of build plans is visible in the VA approved tool.
11. The Contractor shall report status, state and capability of implementation resources and assets and be prepared to discuss their estimated level of work (Story Points), potential risks, dependencies, and necessary Government approval for each build Candidate package. .

The Contractor shall provide a Build/Increment Plan to the COR/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 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, and customer acceptance testing). The Contractor shall include testing related to non-functional requirements, (e.g., load, performance, installation, back-out, and rollback) in the Build Plan. The Contractor shall populate its Test Strategy section of the test plan in VA's implementation of the VA approved tool.

At the conclusion of the Build Planning phase, the Contractor shall provide a Build Plan which includes release planning, the prioritized capabilities, estimation of size and timeline for completion.

**Deliverable:**

A. Build/Increment Plan

### TEST PLANNING (TP) (FFP)

The Contractor shall collaborate with the COR/PM to develop for each release:

1, Review and provide updated information to the TP for each build.

2. Ensure the accurate capture and documentation of all test environments, configuration parameters, administrative accounts and pass codes used for testing. Pass codes shall be documented in the TP in accordance with appropriate security criteria.

3. Develop and document the detailed test data architecture, management and staging procedures to the VA PM for approval in the TP. Details shall include the following information:

a. Queries and updates to data staging
b. Data inputs from all data sources to be validated
c. Data outputs from services to send to consumers
d. Partner data dependencies, processes, and procedures to update and configure data for each environment
e. Develop synthetic test data to mock partner systems and to support performance testing when appropriate
f. POC information and coordination with partners, to capture the required data staging updates

g. Detailed manual and automated processes required to update and maintain test data

4. Determine the appropriateness and validate the feasibility of the testing cadence being planned for integration and performance testing.

5. Document the schedule and scope of each type of test to be conducted at the development level.

6. Develop and maintain in Jira or other approved VA tool, the specific test scripts and test plans for each build. All components should be included in a Release and Build Test Plan. Update to add additional information regarding the status of test and features being tested for each build.

**Deliverable:**

A. Release and Build Test Plan

### 5.5.4 SPRINT PLANNING (FFP)

The Contractor shall:

1. create and prioritize the sprint backlog using the approved prioritized items identified from build planning,.
2. Identify user stories and tasks to be completed within the sprint, the agreement of acceptance criteria for the sprint, and readiness to begin sprint. The sprint design shall define the work and identify the resources required to complete the sprint.
3. Update the VA approved tool to include any additional requirement elaboration details developed during this process.
4. In collaboration with key VA Stakeholders, determine the testing events required for the Sprint.
5. Update requirements traceability in the VA approved tool to demonstrate the linkage between what is being constructed, tested and released in each sprint and the business requirements.
6. Create the Sprint Plan at the conclusion of the Sprint Planning for each Product. 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 delivered in the VA approved tool after being approved by the COR/PM prior to the start of sprint execution.

**Deliverable:**

A. Sprint Plan

### 5.5.5 SPRINT EXECUTION (FFP)

The Contractor shall:

1. Provide a Sprint execution plan and provide a certified Scrum Master to facilitate all ceremonies, ensure the VA approved tool is updated daily, enforce scrum framework, track and assist with removing impediments.
2. Obtain official customer acceptance of the Sprint.
3. Initiate and facilitate a Sprint Retrospective at the end of the Sprint to capture team performance lessons learned. Identify any planned sprint items not completed during the sprint, issues encountered and plans for resolution.

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

1. Sprint Burn Down chart.
2. The Velocity Chart.

**Deliverable:**

A. Sprint Retrospective
B. Sprint Burn Down Chart
C. Velocity Chart

### 5.5.6 TESTING (FFP)

The Contractor shall conduct sprint and build testing as follows:

### TEST DATA (FFP)

The Contractor shall support data seeding and data cleansing (including redaction / masking of Veteran Personally Identifiable Information (PII)) in support of a production scaled test environment.

The Contractor shall create test data that is adequate to conduct both negative and positive test cases and flows across the integrated set of systems for functional validation.

### SPRINT TESTING (FFP)

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 VA Technical Reference Model (TRM).

The Contractor shall follow the Master Test Plan following the templates and data requirements appropriate for each test purpose appropriate to each phase of development. The Contractor shall develop a test plan in the VA approved tool and provide test results for COR/VA PM acceptance.

The Contractor shall support security, accessibility, performance, technical standards, architectural compliance, user acceptance and initial operational capability tests, audits, and reviews and provide results in the VA approved tool. Security scanning is done multiple times throughout the course of a project with multiple methods such as infiltration testing (WASA), code analysis tools (CodeQL, 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.

The Contractor shall develop a Regression test capable of being executed on an ad hoc basis, in the build pipeline, and/or with the nightly build.

The Contractor shall ensure all test and compliance review planning and execution details are included in the Test including version control in the VA approved tool. Specifically test management data and artifacts include such items as scripts, configurations, utilities, tools, plans and results. The Contractor shall ensure that results of all assessments of the project performed by the Contractor or by VA offices are consolidated into the VA approved tool for planning and status reporting.

When a defect is identified during testing, the Contractor shall log it in the VA approved tool, selecting the appropriate severity level. The Contractor shall provide sufficient information to recreate the defect for purposes of analysis and remediation. The Contractor shall support the Project Manager for prioritizing the defect in the sprint backlog. Based on a prioritization the defect could be entered into the current sprint or entered into the backlog.

The Contractor shall ensure data in the VA approved tool is up-to-date on a daily basis so that VA stakeholders can access accurate and timely status.

**Deliverables:**

A. Requirements Traceability Matrix (RTM)

## BUILD ASSEMBLY AND TESTING (FFP)

For products not using Continuous Integration/ Continuous Delivery (CI/CD) (with automated testing and builds), the Contractor shall assemble completed sprints into builds and test the overall build.

The Contractor shall:

1. Support test environment setup including, 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.
2. Support test events as required for each build including:
   a. Product component testing
   b. Component integration and system testing
   c. Quality assurance testing
   d. User acceptance testing
   e. User functionality testing

The Contractor shall test during the build phase and ensure that all the new functionality created in the sprints 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 VA COR/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 and supported by providing Test Results Report to the COR/PM.

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

**Deliverables:**

A. Test Results Report
B. Final Development Code Files, Compiled Code and supporting documentation, as needed

### 5.5.7 RELEASE AND DEPLOYMENT (FFP)

### PRE-RELEASE SUPPORT (FFP)

The Contractor shall support the VA Release process in accordance with current VA processes. The Contractor shall use software industry best practices and VA approved tools to perform CI/CD, continuous coordination and the continuous sharing of knowledge between development and sustainment teams.

The Contractor shall work with the COR/ PM, and stakeholders to develop a PI Planning/Build Release Package for each Product that will outline processes and documentation needed to deploy the build:

1. Develop/update/finalize the 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. The POM shall provide full and detailed descriptions of production operations and maintenance procedures and steps on how to perform production operations and maintenance tasks. The POM shall be kept updated before each release.
2. Develop and maintain the VDD and SDD which is used to identify, maintain, enhance, and recreate the product (IT asset) throughout its lifecycle.
3. 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 ability to access and perform a system function, Technical Manual, System Security Guide, System Contingency Plans, and Disaster Recovery Plan.

**Deliverable:**

A. PI Planning/Build Release Package

### RELEASE AND DEPLOYMENT SUPPORT(FFP/T&M)

Following successful completion of testing, the Contractor shall update and finalize a Technical Documentation Package including software code, materials, manuals, user guides, and release notes and make final, formal delivery to VA for each Product. The Contractor shall be responsible for resolution of any discrepancies.

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 solution and ensure that the architecture is in accordance with VA's architecture guidelines.

The Contractor shall provide subject matter expertise to support and coordinate each release with the VA technical staff and the interfacing product teams and to resolve issues and ensure that migration is completed.

1. Monitor and document the operational solution after release.

In conjunction with the COR, PM and VA designated stakeholders, produce a Release and Deployment Support plan to outline the implementation, deployment, training. release instructions

The Release and Deployment Support Plan and Package shall include updated and final technical documentation:

1. The Solution Deployment Packages (SDP) shall include all applicable required Artifacts covering the Release Management, Product Documentation, and Product Support phases.
2. Updated Production Operations Manual and the deployment, installation, rollback, and back out guide for quick diagnosis of operational problems.
3. Updated technical documentation package.
4. Technical manual that will document the technical design, interactions with other systems, and configuration in the VA Software Library to address changes resulting from an enhancement.
5. Updated Release Notes that describe changes to existing software and new features.

**Deliverable:**

A. Release and Deployment Support Plan and Package
B. Solution Deployment Package (SDP)

### 5.6 SOLUTION ARCHITECTURE AND ADVANCED DATA ENGINEERING (T&M) - OPTIONAL TASK 2)

The Contractor shall support all aspects of the solution architectures for a period of up to 12 months in the Base Period and each Option Period. The aspects and components of the architecture solutions shall comply with VA ASD and PES guidelines and follow reference models set forth by the

VA Enterprise Architecture. The Contractor shall include in the Architectural Solution Design package as part of the SDD following the Demand Management Product Architecture Framework and Ontology:

- Service Capability Architecture
- Service Specification Architecture
- Service Implementation Architecture
- Service Deployment Architecture
- Service Charters
- Logical Data Model
- Data Dictionary
- Data Mapping
- Gap Analysis

The Contractor shall develop a prioritized backlog of architectural/platform requirements with high-priority features identified for near-term builds. The Contractor shall create and maintain enterprise architecture and designs in an iterative manner over the course of sprints and release.

The Contractor shall:

1. Provide, develop, support, and maintain a partner integration guide, clearly defining in the runway how to integrate, interface, consume, and produce services.
2. Manage the enterprise architecture as central to orchestrating technical integration within the applications, as well as with VA and DOD external systems.
3. Deliver an architectural roadmap that defines the to-be design and framework of the solution based on technical improvements and modifications from the original design documented in the SDD.
4. When evaluating the modernization roadmap, a successful team will be capable at evaluating the totality of the Pillar's products and platforms to make informed recommendations on consolidation activities where overlap in capabilities, customer focus, and supported business function occur.
5. Develop and deliver Service Description Documents (SvcDD) describing the interface, integration, and interaction between systems and subsystems. Communication methods and dependencies to other services, and input and output, shall all be defined in the SvcDD
6. Develop and deliver Product Data Definition Models that describe the metadata and the organization of data elements, and standardization of how data elements relate to each other. The data model shall include a detailed description of schemas, data-types, and entities in databases, to include entity relationship diagrams.
7. Develop and deliver VA Product Architecture Framework solution architecture that defines the framework, orchestration, principles, and practices for creating and using the architecture solution; it shall depict models, layers, domains, and views; to include data, information, security, business, information, and delivery of all communications in the architecture.
8. Develop and deliver a style and standard integration guide that details the interface and services patterns to communicate and integrate with other systems.
9. Develop, update, and deliver a System Design Document (SDD) to include:
   A. Updates to the technology stack and TRM software versions
   B. Updates to SDD for every release

C. Submission of an SDD that can be reviewed by ASD, and that will pass an Architecture and Engineering Review Board (AERB) review.

The Contractor shall manage the architecture highlighting both the technical and operational processes and structure across the enterprise. The architecture shall take both existing and planned infrastructure and systems information into account – from the capabilities they currently provide, to the gaps that shall be filled, and the required interfaces to other systems.

**Deliverables:**

A. Architectural Solution Design package
B. Service Description Documents (SvcDDs)
C. Product Data Definition Models
D. VA Product Architecture Framework
E. Architectural Roadmap | Runway
F. System Design Documents (SDD)

## 5.7 OPERATIONS & MAINTENANCE SERVICES (OPTIONAL TASKS 3-7) (FFP)

The Contractor shall provide Spike, Small, Medium, Large Scrum, or Multi-Scrum teams to support all O&M services and deliverables identified in Section 4.6.1, including all subparagraphs. O&M Scrum teams shall provide ongoing support related to the performance of routine, preventive, predictive, scheduled, and unscheduled actions to aimed at preventing system/production failure (i.e., break/fix) and correcting software defects. with the goal of increasing efficiency and reliability on a continuous basis. VA systems are constantly evolving to intake new applications/systems that will require sustainment support to meet VA priorities. The scrum team size to be exercised will consider the size/complexity of the required tasks. Examples of task size/complexity to be considered are provided below:

### 5.7.1 OPERATIONS & MAINTENANCE SUPPORT - SPIKE SCRUM TEAM (OPTIONAL TASK 3)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 75 teams at minimum 1 months and a maximum of 3 months of performance per team (i.e.., 75 total months).

### 5.7.2 OPERATIONS & MAINTENANCE SUPPORT - SMALL SCRUM TEAM (OPTIONAL TASK 4)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 30 teams at 1 months and maximum 12 months of performance per team (i.e., 360 total months).

### 5.7.3 OPERATIONS & MAINTENANCE SUPPORT - STANDARD SCRUM TEAM (OPTIONAL TASK 5)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 20 teams at a minimum of 1 months and maximum 12 months of performance per team (i.e., 240 total months).

### 5.7.4 OPERATIONS & MAINTENANCE SUPPORT - LARGE SCRUM TEAM (OPTIONAL TASK 6)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 20 teams at 1 months and maximum 12 months of performance per team (i.e., 240 total months).

### 5.7.5 OPERATIONS & MAINTENANCE SUPPORT – MULTI-SCRUM TEAM (OPTIONAL TASK 7)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 15 multi-teams at minimum of 1 months and maximum 12 months of performance per team (i.e., 180 total months).

## 5.8 DEVELOPMENT SERVICES (OPTIONAL TASKS 8-11) (FF)

The Contractor shall provide a scrum team to support all the services and deliverables identified in Section 5.5, including all subparagraphs. Development scrum teams shall support system development, enhancements and/or modernization from the product backlog as determined by VA Product/Project business owners. VA systems are constantly evolving to intake new applications/systems that will require development support to meet VA priorities. 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 scrum team size to be exercised will consider the size/complexity of the required tasks. Examples of task size/complexity to be considered are provided below:

| Task Size / Complexity | Description |
|---|---|
| Spike | The Contractor shall provide a scrum team consisting of a minimum of 2 FTE and a maximum of 4 FTE resources per team to support all services/deliverables required by PWS 5.2 (O&M), PWS 5.3 (CDW Support), PWS 5.4 (VINCI Support) or PWS 5.5 (Development), including all subparagraphs. A Spike Scrum Team is appropriate for short, focused activity by individuals with senior or specific skills, as needed. |
| Small | System efficiency improvements; minor to moderate enhancements to existing processes. Updating existing letters, forms, reports or correspondence protocols, and new API. Moderate to major user interface updates. |

| | |
|---|---|
| | Additions/modifications/deletions to 3 to 8 data fields in an information service (and corresponding adapter, access, and/or partner component). Minor user interface changes or API if applicable, reference table updates, data validation enhancements, minor updates to existing business rules or existing services, additions/modifications/deletions to 2 or less data fields in an information service (and corresponding adapter). |
| Medium | Minor to moderate enhancements, major business rule additions or rewrites, extensive database modifications or major modifications to existing services, new letters, forms, reports, or correspondence protocols, 1-2 new SOA components (Presentation, Process, Information, Business Application, Access, Partner, Infrastructure levels), integration with new system, system modifications to propagate/seed/synchronize authoritative data to/from a source where a propagation or seeding exists. Orchestrations with 1-2 non- dependencies. Additions / modifications / deletions to 9 data fields in an information service (and corresponding adapter, access, and/or partner component), Development of new web services requiring 1-2 component levels. |
| Large | Development of new web services or APIs requiring 3-5 or more component (logic layer, service layer, infrastructure layer, or partner layer) levels, or extensive system modifications to propagate/seed/synchronize authoritative data to/from a new service, orchestrations with 3-5 dependencies. Development of new web services or APIs requiring 5 or more component levels and 2+ integrations, orchestrations with 6 or more dependencies, major system enhancements impacting multiple systems/services. |

### 5.8.1 DEVELOPMENT - SPIKE SCRUM TEAM (OPTIONAL TASK 8)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 75 teams at minimum 1 months  and a maximum of 3 months of performance per team (i.e.., 75 total months).

### 5.8.2 DEVELOPMENT – SMALL SCRUM TEAM (OPTIONAL TASK 9)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 30 teams at a minimum of 1 months and maximum 12 months of performance per team (i.e., 360 total months max).

### 5.8.3 DEVELOPMENT - STANDARD SCRUM TEAM (OPTIONAL TASK 10)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 20 teams at a minimum of 1 months and maximum 12 months of performance per team (i.e., 240 total months maximum).

### 5.8.4 DEVELOPMENT – LARGE SCRUM TEAM (OPTIONAL TASK 11)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 20 teams at a minimum of 1 months and maximum 12 months of performance per team (i.e., 240 total months maximum).

### 5.8.5 DEVELOPMENT – MULTI-SCRUM TEAM (OPTIONAL TASK 12)

During the Base Period and each Option Period, this Optional Task may be exercised for up to 15 multi-teams at minimum of 1 months and maximum 12 months of performance per team (i.e., 180 total months).

### 5.8.6 CDW SQL SERVER ANALYSIS SERVICES (SSAS) SUPPORT SERVICES (OPTIONAL TASK 13)

The Contractor shall develop and maintain approximately eight CDW level On Line Analytical Processing (OLAP) cubes per year. These cubes would have on the order of 100 million fact table rows and contain on the order of 10-15 dimensions. The Contractor shall us Data Domain ETL Script Implementation Document SSAS 2014 (or later) for cube development. The Contractor shall use the SSAS tool suite to design, develop, and implement cubes that are based upon CDW data.

The Contractor shall provide a SSAS Cube Design Document for each cube. This document shall contain a SSAS cube project overview, business sponsor, and the Star Schema that contains all Facts, Dimensions, Measures, and Dimensional Hierarchies.

### 5.8.7 CDW MICROSOFT POWERBI SUPPORT SERVICES (OPTIONAL TASK 14)

The Contractor shall develop and maintain approximately five enterprise scale CDW level PowerBI reporting projects per year. These projects shall assimilate data from the CDW, either in the form of relational data or OLAP cubes, to assess the feasibility of leveraging the PowerBI suite of tools for internal business intelligence reporting needs. The Contractor shall design the look and feel of the reports using the PowerBI tool with input from end user representatives. The Contractor shall use the PowerBI suite to design, develop, and implement reports. The Contractor shall provide a PowerBI Report Implementation Document for each assigned project that includes a project summary and a list of reports that are part of the project.

## 5.9 OUTGOING TRANSITION SUPPORT (OPTIONAL TASK 15)

The Contractor shall provide a plan for 90 days of outgoing transition support for transitioning work from the current TO to a follow-on TO or Government entity. This Transition Plan shall include, but is not limited to:

1. Coordination with Government representatives.
2. Review, evaluation and transition of current support services.
3. Transition of historic data to new Contractor system.
4. Disable access to VA approved tool accounts.

5. Transfer of hardware and software warranties, maintenance agreements and licenses.
6. Transfer of all necessary business and/or technical documentation.
7. Orientation phase and program to introduce Government and Contractor personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes.
8. Disposition of Contractor purchased Government owned assets.
9. Turn in of all Government keys, ID/access cards, and security codes.
10. Transition of all programing source codes, source documents, and associated operations and maintenance procedure documents.
11. Provide transition plan, project management transition documents, technical management transition documents.
12. Provide project technical, and operations and maintenance procedure transition training.

**Deliverable:**

A. Transition Plan
B. Programming source code
C. Transition documents
D. Transition training

## 6.0 GENERAL REQUIREMENTS

### 6.1 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 | 1. Shows understanding of requirements<br>2. Efficient and effective in meeting requirements<br>3. Meets technical needs and mission requirements<br>4. Provides quality services/products as measured by number of defects identified in each stage of testing and production and by results of SonarQube/Fortify scans. | Maintainability Rating <= 5%; Issues < 5 (severity minor); Security Rating = 0; reliability rating = 0 |
| B. Project Milestones and Schedule | 1. Quick response capability<br>2. Products completed, reviewed, delivered in accordance with the established schedule | Satisfactory or higher |

| Performance Objective | Performance Standard | Acceptable Levels of Performance |
|---|---|---|
| | 3. Notifies customer in advance of potential problems | |
| C. Cost & Staffing | 1. Currency of expertise and staffing levels appropriate<br>2. Personnel possess necessary knowledge, skills and abilities to perform tasks | Satisfactory or higher |
| D. Management | 1. Integration and coordination of all activities to execute effort | Satisfactory or higher |

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

## 6.2 SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

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

### 6.2.1 SECTION 508 STANDARDS

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: **.** 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, contractor may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, 1194.5. Such contractors 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.

### 6.2.2 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.

### 6.2.3 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 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.

**Deliverable:**

A. Final Section 508 Compliance Test Results

## 6.3 ORGANIZATIONAL CONFLICT OF INTEREST

All functions related to Acquisition Support shall be on an advisory basis only. Please be advised that since the awardee of this TO will provide systems engineering, technical direction, specifications, work statements, and evaluation services, some restrictions on future activities of the awardee may be required in accordance with FAR 9.5 and the clause entitled, Organizational Conflict of Interest, found in Section H of the T4NG basic contract. The Contractor and its employees, as appropriate, shall be required to sign Non-Disclosure Agreements (Appendix A).

## ADDENDUM B- VA INFORMATION AND INFORMATION SYSTEM SECURITY / PRIVACY LANGUAGE

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

### B.1 GENERAL

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

### B.2 ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

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

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

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

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

## B.3 VA INFORMATION CUSTODIAL LANGUAGE

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

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

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

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

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

f. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

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

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

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

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

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

## B.4 INFORMATION SYSTEM DESIGN AND DEVELOPMENT

a. Information systems that are designed or developed for or on behalf of VA at non -VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* and the *TIC Reference Architecture*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

b. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA.

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

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

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

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

g. The Contractor/Subcontractor agrees to:

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

(a) The Systems of Records (SOR); and

(b) The design, development, or operation work that the Contractor/Subcontractor is to perform.

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

3) Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

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

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

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

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

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

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 issue shall be remediated as quickly as is practical, based on 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 requirements identified within the TO.

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

## B.5 INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

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

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

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

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

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

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

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

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

1) Vendor must accept the system without the drive;

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

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

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

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

(b) Any fixed hard drive on the device must be nondestructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

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

## B.6 SECURITY INCIDENT INVESTIGATION

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

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

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

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

## B.7 LIQUIDATED DAMAGES FOR DATA BREACH

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

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

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

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

(a) date of occurrence.

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

3) Number of individuals affected or potentially affected.

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

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

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

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

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

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

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

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

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

1) Notification.

2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports.

3) Data breach analysis.

4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution.

5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and

6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

## B.8 SECURITY CONTROLS COMPLIANCE TESTING

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

## B.9 TRAINING

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

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

2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course and complete this required privacy and information security training annually.

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

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

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

## APPENDIX A

# CONTRACTOR NON-DISCLOSURE AGREEMENT

This Agreement refers to Contract/Order _________________ entered into between the Department of Veterans Affairs and _________________________ (Contractor).

**As an officer of *<fill in name of Contractor>*, authorized to bind the company, I understand that in connection with our participation in the *<fill in program>* acquisition under the subject Contract/Order, Contractor's employees may acquire or have access to procurement sensitive or source selection information relating to any aspect of *<fill in program>* acquisition. Company *<fill in name>* hereby agrees that it will obtain Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements from any and all employees who will be tasked to perform work under the subject Contract/Order prior to their assignment to that Contract/Order. The Company shall provide a copy of each signed agreement to the Contracting Officer. Company *<fill in name>* acknowledges that the Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements require Contractor's  employee(s) to promptly notify Company management in the event that the employee releases any of the information covered by that agreement and/or whether during the course of their participation, the employee, his or her spouse, minor children or any member of the employee's immediate family/household has/or acquires any holdings or interest whatsoever in any other private organization (e.g., contractors, contractors, their subcontractors, joint venture partners, or team members), identified to the employee during the course of the employee's participation, which may have an interest in the matter the Company is supporting pursuant to the above stated Contract/Order. The Company agrees to educate its employees in regard to their conflict of interest responsibilities.**

Company ***<fill in name>*** further agrees that it will notify the Contracting Officer within 24 hours, or the next working day, whichever is later, of any employee violation. The notification will identify the business organization or other entity, or individual person, to whom the information in question was divulged and the content of that information. Company ***<fill in name>*** agrees, in the event of such notification, that, unless authorized otherwise by the Contracting Officer, it will immediately withdraw that employee from further participation in the acquisition until the Organizational Conflict of Interest issue is resolved.

This agreement shall be interpreted under and in conformance with the laws of the United States.

____________________________________ ____________________________________
Signature and Date                                        Company

____________________________________
____________________________________

Printed Name Phone Number

## CONTRACTOR EMPLOYEE PERSONAL FINANCIAL INTEREST/PROTECTION OF SENSITIVE INFORMATION AGREEMENT

This Agreement refers to Contract/Order ____________________ entered into between the Department of Veterans Affairs and ___________________ (Contractor).

As an employee of the aforementioned Contractor, I understand that in connection with my involvement in the support of the above referenced Contract/Order, I may receive or have access to certain “sensitive information” relating to said Contract/Order, and/or may be called upon to perform services which could have a potential impact on the financial interests of other companies, businesses or corporate entities. I hereby agree that I will not discuss or otherwise disclose (except as may be legally or contractually required) any such “sensitive information” maintained by the Department of Veterans Affairs or by others on behalf of the Department of Veterans Affairs, to any person, including personnel in my own organization, not authorized to receive such information.

“Sensitive information” includes:

(a) Information provided to the Contractor or the Government that would be competitively useful on current or future related procurements; or

(b) Is considered source selection information or bid and proposal information as defined in FAR 2.101, and FAR 3.104-4; or

(c) Contains (1) information about a Contractor’s pricing, rates, costs, schedule, or contract performance; or (2) the Government’s analysis of that information; or

(d) Program information relating to current or estimated budgets, schedules or other financial information relating to the program office; or

(e) Is properly marked as source selection information or any similar markings.

Should “sensitive information” be provided to me under this Contract/Order, I agree not to discuss or disclose such information with/to any individual not authorized to receive such information. If there is any uncertainty as to whether the disclosed information comprises “sensitive information”, I will request my employer to request a determination in writing from the Department of Veterans Affairs Contracting Officer as to the need to protect this information from disclosure.

I will promptly notify my employer if, during my participation in the subject Contract/Order, I am assigned any duties that could affect the interests of a company, business or corporate entity in which either I, my spouse or minor children, or any member of my immediate family/household has a personal financial interest. “Financial interest” is defined as compensation for employment in the form of wages, salaries, commissions, professional fees, or fees for business referrals, or any financial investments in the business in the form of direct stocks or bond ownership, or partnership interest (excluding non-directed retirement or other mutual fund investments). In the event that, at a later date, I acquire actual knowledge of such an interest or my employer becomes involved in proposing for a solicitation resulting from the work under this Contract/Order, as either a contractor, an advisor to a contractor, or as a Subcontractor to a contractor, I will promptly notify my employer. I understand this may disqualify me from any further involvement with this Contract/Order, as agreed upon between the Department of Veterans Affairs and my company.

Among the possible consequences, I understand that violation of any of the above conditions/requirements may result in my immediate disqualification or termination from working on this Contract/Order pending legal and contractual review.

I further understand and agree that all Confidential, Proprietary and/or Sensitive Information shall be retained, disseminated, released, and destroyed in accordance with the requirements of law and applicable Federal or Department of Veterans Affairs directives, regulations, instructions, policies and guidance.

This Agreement shall be interpreted under and in conformance with the laws of the United States.

I agree to the Terms of this Agreement and certify that I have read and understand the above Agreement. I further certify that the statements made herein are true and correct.

_______________________________________________

_______________________________________________

Signature and Date                    Company

_______________________________________________

_______________________________________________

Printed Name                    Phone Number