

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

**FINANCIAL SERVICES CENTER (FSC)**

**INFORMATION TECHNOLOGY OPERATIONS SUPPORT**

**Date:** 29 November 2023

VA-24-00018197

**PWS Version Number:** 0.2

Contents

[1.0 BACKGROUND 4](#_Toc151728404)

[2.0 APPLICABLE DOCUMENTS 5](#_Toc151728405)

[3.0 SCOPE OF WORK 8](#_Toc151728406)

[3.1 APPLICABILITY 9](#_Toc151728407)

[3.2 ORDER TYPE 10](#_Toc151728408)

[3.3 DESCRIPTION OF CURRENT TECHNICAL ENVIRONMENT 10](#_Toc151728409)

[3.3.1 VA FSC IT SOFTWARE INFRASTRUCTURE 10](#_Toc151728410)

[4.0 PERFORMANCE DETAILS 16](#_Toc151728411)

[4.1 PERFORMANCE PERIOD 16](#_Toc151728412)

[4.2 PLACE OF PERFORMANCE 16](#_Toc151728413)

[4.3 TRAVEL 17](#_Toc151728414)

[5.0 SPECIFIC TASKS AND DELIVERABLES 18](#_Toc151728415)

[5.1 PROGRAM MANAGEMENT 19](#_Toc151728416)

[5.1.1 TRANSITION-IN SUPPORT 20](#_Toc151728417)

[5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN 20](#_Toc151728418)

[5.1.3 REPORTING REQUIREMENTS 20](#_Toc151728419)

[5.1.4 TECHNICAL KICKOFF MEETING 21](#_Toc151728420)

[5.1.5 CONTRACTOR PERSONNEL REQUIREMENTS 22](#_Toc151728421)

[5.1.6 TRAINING 22](#_Toc151728422)

[5.1.7 FACILITY REQUIREMENTS 23](#_Toc151728423)

[5.1.7.1 PHYSICAL SECURITY REQUIREMENTS 23](#_Toc151728424)

[5.1.7.2 FSC ACCESS PRIVILEGES 24](#_Toc151728425)

[5.1.7.3 EMERGENCY SERVICE 25](#_Toc151728426)

[5.1.8 PROFESSIONAL STANDARDS REQUIREMENTS 25](#_Toc151728427)

[5.1.9 TRIP REPORTING 27](#_Toc151728428)

[5.1.10 ACTIVITY-BASED COSTING LABOR TRACKING 27](#_Toc151728429)

[5.2 FTS OPERATIONS AND MAINTENANCE SUPPORT 27](#_Toc151728430)

[5.2.1 TECHNICAL WRITING 28](#_Toc151728431)

[5.2.2 DISASTER RECOVERY ANALYSIS AND SUPPORT 29](#_Toc151728432)

[5.2.3 INFRASTRUCTURE SUPPORT 30](#_Toc151728433)

[5.2.3.1 SYSTEMS ADMINISTRATION SERVICES 30](#_Toc151728434)

[5.2.3.2 NETWORK ADMINISTRATION SERVICES 32](#_Toc151728435)

[5.2.3.3 DATABASE ADMINISTRATION SERVICES 33](#_Toc151728436)

[5.2.3.4 CYBERSECURITY 35](#_Toc151728437)

[5.2.3.5 IT SERVICE DESK 39](#_Toc151728438)

[5.2.4 APPLICATION PRODUCTION SUPPORT AND MAINTENANCE SERVICES 42](#_Toc151728439)

[5.2.5 ENTERPRISE CONTENT MANAGEMENT (ECM) APPLICATION AND ADMINISTRATION SERVICES 43](#_Toc151728440)

[5.2.6 SCANNING SUPPORT 44](#_Toc151728441)

[5.2.7 SYSTEM ENGINEERING 45](#_Toc151728442)

[5.2.8 CLOUD SYSTEM ENGINEERING 47](#_Toc151728443)

[5.2.9 ENTERPRISE ARCHITECTURE STRATEGY SUPPORT 50](#_Toc151728444)

[5.2.10 SOLUTION ARCHITECTURE IMPACT ASSESSMENT SUPPORT 51](#_Toc151728445)

[5.2.11 ORGANIZATIONAL ARCHITECTURE SUPPORT 52](#_Toc151728446)

[5.2.12 SYSTEMS ANALYSIS SUPPORT 54](#_Toc151728447)

[5.2.13 EDI HELP DESK/OPERATIONS SUPPORT SERVICES 55](#_Toc151728448)

[5.2.14 EDI APPLICATION SUPPORT 55](#_Toc151728449)

[5.3 DATA ANALYTICS SUPPORT 57](#_Toc151728450)

[5.3.1 DATA ANALYSIS AND BUSINESS INTELLIGENCE 57](#_Toc151728451)

[5.3.2 DATA ANALYTICS CUSTOMER SUPPORT 60](#_Toc151728452)

[5.3.3 DATA MANAGEMENT AND GOVERNANCE 61](#_Toc151728453)

[5.4 PRIVACY SERVICE 62](#_Toc151728454)

[5.5 TRANSITION-OUT SUPPORT (OPTIONAL TASK) 64](#_Toc151728455)

[6.0 GENERAL REQUIREMENTS 65](#_Toc151728456)

[6.1 ENTERPRISE AND IT FRAMEWORK 65](#_Toc151728457)

[6.1.1 VA TECHNICAL REFERENCE MODEL 65](#_Toc151728458)

[6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 65](#_Toc151728459)

[6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6) 67](#_Toc151728460)

[6.1.4 TRUSTED INTERNET CONNECTION (TIC) 67](#_Toc151728461)

[6.1.5 STANDARD COMPUTER CONFIGURATION 67](#_Toc151728462)

[6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM) 68](#_Toc151728463)

[6.1.7 PROCESS ASSET LIBRARY (PAL) 68](#_Toc151728464)

[6.1.8 SOCIAL SECURITY NUMBER (SSN) REDUCTION 68](#_Toc151728465)

[6.2 SECURITY AND PRIVACY REQUIREMENTS 69](#_Toc151728466)

[6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 69](#_Toc151728467)

[6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 70](#_Toc151728468)

[6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 71](#_Toc151728469)

[6.4 PERFORMANCE METRICS 72](#_Toc151728470)

[6.5 FACILITY/RESOURCE PROVISIONS 73](#_Toc151728471)

[6.6 GOVERNMENT FURNISHED PROPERTY 74](#_Toc151728472)

[ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 75](#_Toc151728473)

[ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 80](#_Toc151728474)

# BACKGROUND

The U.S. Department of Veterans Affairs (VA) continues its pursuit to make America’s Veterans a priority; to serve and honor the men and women who are America’s Veterans. VA is committed to five core values that define “who” we are and how we care for Veterans. The core values are Integrity, Commitment, Advocacy, Respect, and Excellence.

The VA Financial Services Center (FSC) is a Franchise Fund site authorized pursuant to the Government Management Reform Act of 1994 (Public Law 103-356). The Act authorizes designated agencies to provide certain common administrative support services on a reimbursable basis both internally and to other Government agencies. Permanent status was conferred upon the VA Franchise Fund under the “Military Quality of Life and Veterans Affairs Appropriations Act, 2006,” Public Law 109-114. Consequently, the VA FSC receives no federally appropriated funding and is required to market VA FSC services to customers. As such, the VA FSC provides financial services to VA as well as other government agencies (OGAs).

The mission of the VA FSC Financial Technology Service (FTS) is to provide high-quality IT infrastructure, software engineering, including system and data, Architecture, Electronic Commerce (EC)/Electronic Data Interchange (EDI) (EC/EDI), and system and database support services to the FSC in support of the FSC's overall mission of providing high-quality financial services, exceeding the expectations of our Federal customers, inspiring their trust and empowering them to focus on their core missions.

VA FSC Data Analytics Service (DAS) is dedicated to creating, promoting, encouraging, and advancing a full range of analytical tools. These tools drive evidence-based program decisions, cost savings, process improvements, identification of fraud, waste, and abuse, budget forecasts, and management efforts to drive innovation. Analytical tools aid in efficient delivery of VA programs that ensure Congressional funding is utilized to a level that honors the commitment of VA, which in turn ensures VA continues meeting the mission to make the Veterans a priority for the Nation. DAS offers financial monitoring tools and analytics which drive technological solutions to help propel the responsible use of the Nation’s VA hospitals and facilities to ensure that our Veterans, and their families, are cared for and provide for a resilient future.

In November 2018, VA issued the Cloud First Policy mandating that all new and existing IT solutions be assessed to determine suitability to be offered as an enterprise cloud computing service. The VA Enterprise Cloud (VAEC) was established by the Enterprise Cloud Solutions Office (ECSO) in 2017, to host cloud computing solutions. VA anticipates that solutions shall be deployed in the VAEC as defined in VA’s Use of the VAEC to Host Solutions and Use of Cloud-Based Native Technologies and Approaches Policies.

# APPLICABLE DOCUMENTS

1. VA Enterprise Cloud Technical Reference Guide, Version 1.3 July 2018
2. VA Cloud-First Policy, November 15, 2016
3. Use of the VA Enterprise Cloud (VAEC) to Host Solutions, January 16, 2018
4. Use of Cloud-Based Native Technologies and Approaches, April 10, 2018
5. The Health Information Technology for Economic and Clinical Health Act (HITECH) Act (https://www.govinfo.gov/content/pkg/PLAW-111publ5/html/PLAW-111publ5.htm)
6. Electronic Communications Privacy Act of 1986: (https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg1848.pdf)
7. 44 U.S.C. § 3541-3549, “Federal Information Security Management Act (FISMA) of 2002”
8. “Federal Information Security Modernization Act of 2014”
9. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”
10. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
11. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
12. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
13. 10 U.S.C. § 2224, "Defense Information Assurance Program"
14. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
15. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
16. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
17. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <https://www.va.gov/vapubs/index.cfm>
18. VA Handbook 0710, “Personnel Security and Suitability Program,” May 2, 2016, <https://www.va.gov/vapubs/index.cfm>
19. VA Directive and Handbook 6102, “Internet/Intranet Services,” August 5, 2019
20. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” January 18, 2017
21. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
22. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
23. NIST SP 800-66 Rev. 1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” October 2008
24. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
25. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
26. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021
27. VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021
28. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” March 12, 2019
29. VA Handbook 6500.5, “Incorporating Security and Privacy into the System Development Lifecycle,” March 22, 2010
30. VA Handbook 6500.6, “Contract Security,” March 12, 2010
31. VA Handbook 6500.8, “Information System Contingency Planning,” April 6, 2011
32. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018
33. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
34. 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>
35. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)
36. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
37. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
38. VA Handbook 6510, “VA Identity and Access Management,” January 15, 2016
39. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
40. VA Directive 6300, “Records and Information Management,” September 21, 2018
41. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010
42. 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
43. 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)
44. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
45. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
46. 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
47. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
48. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
49. 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>)
50. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
51. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” updated March 02, 2020
52. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
53. NIST SP 800-164, “Guidelines on Hardware-Rooted Security in Mobile Devices (Draft),” October 2012
54. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981, “Mobile, PIV, and Authentication,” March 2014
55. 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>)
56. 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>)
57. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>
58. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, <https://www.cisa.gov/publication/tic-30-core-guidance-documents>
59. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
60. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
61. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
62. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
63. Executive Order 13834, “Efficient Federal Operations,” dated May 17, 2018
64. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
65. VA Directive 0058, “VA Green Purchasing Program,” July 19, 2013
66. VA Handbook 0058, “VA Green Purchasing Program,” July 19, 2013
67. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
68. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
69. “Veteran Focused Integration Process (VIP) Guide 4.0,” January 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
70. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
71. “DevSecOps Product Line Management Playbook” version 2.0, May 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>
72. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
73. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
74. Social Security Number (SSN) Fraud Prevention Act of 2017
75. Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018

# SCOPE OF WORK

The Contractor shall provide on-site professional services to support the FSC FTS, Data Analytics Service (DAS), and its current and future Divisions and Branches. Current FTS branches are Operations and Maintenance (OMD), IT Business Operations Division (ITBOD), Program Management Office (PMO), and Financial Management Business Transformation (FMBT). Additionally, the Contractor shall provide support of the FSC IT infrastructure, operations, projects, and various initiatives supported by FSC on behalf of VA and OGAs. The current technical environment to be supported is described in PWS section 3.3.

The Contractor shall provide support services and develop deliverables for all FSC projects including new software projects, maintenance releases, and emergency software releases. Services and workload will support FSC’s current and potential projects which are both internal to FSC and external projects for other VA customers and potentially other Government entities. The Contractor shall support projects which frequently include, but are not limited to, the following core business areas: financial management, fraud, waste, and abuse, supply chain, category management, purchase card, internal compliance management, acquisition obligations, healthcare, travel, and other initiatives.

All deliverables shall align with the Veterans-Focused Integration Process (VIP). The Contractor shall perform resource planning in support of new software projects, maintenance releases, emergency software releases, and operations and maintenance support. The Contractor shall manage resource levels and coordinate with FSC Project Managers and FTS management, as needed, to understand schedule timelines.

Technical Writing support may be allocated to divisions other than OMD and HPO upon Contracting Officer’s Representative (COR) approval to support surges in activity.

The scope of services required includes the following functional areas and tasks:

a. Infrastructure Support

b. Desktop/ Help Desk Services

c. Application Production Support and Maintenance Services

d. Technical Writer Support

e. Enterprise Architecture (EA)

f. Data Modeling

g. Project Support

h. Systems Analysis

i. Enterprise systems administration and integration

j. Systems Administration

k. Storage and backup Administration

l. Application Administration

m. Information Assurance

n. Web Application Security Assessment (WASA)

p. Cybersecurity

n. Privacy Services

o. Data Management

p. Database Design

q. Database Administration

r. System Design

s. System Engineering

t. Capacity Planning

u. Network design

v. Network administration

w. Cloud solution design and administration

x. Support for Cloud-based systems, software, or applications

y. Internal Security Monitoring & Alerting (ISMA)

z. Threat Intelligence & Modeling (TIM)

aa. Support for Managed Service providers including but not limited to:

1. Software as a Service (SaaS)

ii. Platform as a Service (PaaS)

iii. Infrastructure as a Service (IaaS)

iv. Database as a Service (DaaS)

bb. Support for migrating systems and applications from on-premises to a Cloud solution

cc. Disaster Recovery (DR) and Information System Contingency Planning (ISCP) support

dd. EDI Technical Support

ee. EDI Administrative and Business Analysis

## APPLICABILITY

This Task Order (TO) effort PWS is within the scope of paragraph(s) 4.1.2: Standards, Policy, Procedure and Process Development, and Implementation Support, 4.1.4: Technology Refresh and Configuration Reviews, 4.1.6: Program Management Support, 4.6.1: Systems/Network Administration, 4.6.2: Network and Telecommunications Infrastructures, 4.9: Operations and Maintenance, and 4.10: Training of the T4NG Basic PWS.

## ORDER TYPE

The effort shall be proposed on a Time and Materials (T&M) basis with a Cost Reimbursable Travel line item.

## DESCRIPTION OF CURRENT TECHNICAL ENVIRONMENT

Following is an overview of the current VA-FSC IT Infrastructure and Technical Environment:

## 3.3.1 VA FSC IT SOFTWARE INFRASTRUCTURE

Following is an overview of the current VA-FSC IT Infrastructure and Technical Environment:

The VA-FSC IT Software Infrastructure consists, but is not limited to, the following products:

1. Microsoft Desktop and Server Operating Systems

2. Microsoft Office products such as Word, Excel, PowerPoint, Project, Visio, Outlook, Office 365

3. Active Directory

4. Structured Query Language (SQL)

5. SQL Server Reporting Services (SSRS)

6. SQL Management Studio

7. SQL Server Data Tools

8. Storage Area Network software

9. Red Hat Enterprise Linux (RHEL) Operating Systems and Products

10. Other client and server software

11. Rightfax

12. TeamMate

13. Data Bricks

14. Informatica

15. Tibco Instream Validator

16. Oracle HTTP server

17. Jenkins

18. Pega

19. Adobe

20. Power BI

21. Tableau

22. Excel PowerPivot

23. R Software

24. RS Studio

25. Python

26. HD Insight

27. JBOSS

28. Tomcat

29. Business Activity Model BAM

30. Visual Studio .Net development environment

31. Internet Information Services (IIS)

32. SharePoint

33. Dynamics – CRM, Great Plains

34. Team Foundation Server

35. System Center

36. Pega Business Process Management (BPM)

37. IBM FileNet P8

38. Oracle Database

39. Oracle Service-Oriented Architecture (SOA)

40. Oracle Enterprise Service Bus (ESB)

32. Oracle WebLogic

41. Plexis Claims Manager

42. Electronic Claims Adjudication Management System (eCAMS)

43. VMWare

44. Citrix XenDesktop

45. Thin Clients

46. Checkfree

47. Kofax Ascent Capture

48. Kofax Accounts

49. VL Trader

50. TrustedLink Enterprise (TLE)

51. MuleSoft

52. LINUX Openshift

53. Kubernetes

54. Instream HIPAA validator

55. Vitria BusinessWare

56. Microsoft Azure

57. Robotics Automation

58. Machine Learning

59. Amazon Web Services (AWS)

60. Ansible

61. Centrify

62. JAVA

63. Vectra AI

64. SIEM Tool

**3.3.2 VA FSC IT IN-HOUSE DEVELOPED APPLICATIONS**

The VA-FSC currently provides production support and maintenance for over 100 in-house developed applications and reporting systems, which were created with Microsoft Visual Studio, Eclipse, and Pega BPM development tools. VA estimates that this will increase over the life of this Task Order. Most of these applications include custom code and Commercial Off the Shelf (COTS) software.

**3.3.3 VA FSC IT HARDWARE INFRASTRUCTURE**

The VA-FSC IT hardware infrastructure primary resides in two VA enduring data centers and consists of:

1. Physical Servers

1. Austin, TX – The Austin Information Technology Center (AITC) facility currently has over 100 physical servers mostly hosting over 1000 VMWare virtual servers.

2. Philadelphia, PA– The back-up facility is at the Philadelphia Information Technology Center (PITC) and currently has over 30 physical servers hosting over 100 VMWare virtual servers to be used in a disaster recovery (DR) situation.

B. Storage Area Network (SAN) – The FSC’s Storage Area Network (SAN) with total storage at approximately four (4) Petabytes (PB) combined between the two above locations.

C. Over 1500 PCs. A workstation PC can be either a desktop PC or a notebook PC.

D. Approximately 20 Multi-Function devices for printing, scanning, faxing, and copying; and various other network and stand-alone printers.

E. Two (2) IBML ImageTrac high-speed scanners.

**3.3.4 VA FSC LOCAL AREA NETWORK**

The VA-FSC local area network (LAN):

A. Consists of primarily Cisco routers and switches with some F5 load balancing appliances within each data center location.

B. Connects to the Internet and to the VA intranet via a redundant pair of VA supplied network connections.

**3.3.5 VA EC/EDI ENVIRONMENTS**

The following provides overview information about the VA Gentran EC/EDI environment:

a. Is comprised of the Sterling Gentran for Multiple Virtual Storage (MVS) version 6.5 software, which is installed on an IBM z/900.

b. The translated data interfaces with multiple mainframe based legacy applications, such as the VA Financial Management System (FMS), the VA Personnel and Accounting Integrated Data (PAID), the VA-FSC Document Management System (DMS), and the VA Data Management Interface (DMI) and server based software, such as the Instream HIPAA validation tool and TrustedLink Enterprise

c. The mainframe legacy applications are written in COBOL and the server-based applications are written in Microsoft .Net or Visual Studio environment. The following are applications maintained by the FSC:

1. **e-Claims** application processes flat file medical insurance claims received in Austin from the VA medical centers. These claims are translated into a compliant ASC X12 837 transaction and sent over a dedicated connection to a clearinghouse. The clearinghouse forwards the ASC X12 837s on to the payers following internal business rules. The VA currently sends out secondary claims for processing to the clearinghouse. The determination is made at the FSC, by referring to a table of payers accepting electronic secondary claims, whether the secondary claim is to be processed electronically by the clearinghouse, or printed and mailed to the payers. All transactions received from the medical centers, via MailMan, are processed into the DMI system or extraction by the application. FSC IT staff are currently working on the processes and procedures to establish a second clearinghouse to process X12 837 transactions.

2. **e-MRA** (Medicare Remittance Advice) application processes the electronic ASC X12 835 transactions received in Austin from the clearinghouse. As the VA is not paid by Medicare, to create a secondary claim with the Medicare allowable information, the VA has contracted with an independent vendor to process the VA primary Medicare claims and return the allowed/disallowed information. The Accredited Standards Committee (ASC) X12 835 is translated by the FSC and sent to the VA medical centers for processing. The information is used in creating the secondary claim for Veterans having additional medical coverage. All transactions sent to the medical centers, via MailMan, are processed into the DMI system by the application.

3. **e-Reports** applicable application provides a customer a series of reports related to the processing of electronic transactions in support of the Veterans Health Administration (VHA) Medical Care Collection Fund (MCCF) activities.

4. **e-Payments** application processes the electronic ASC X12 835 electronic remittance advice (ERA) transactions and ASC X12 835 electronic fund transfers (EFT) transactions received in Austin from the clearinghouse. These transactions are translated by the FSC to a flat-file format and sent to the VA medical centers for processing. All transactions sent to the medical centers, via MailMan, are processed into the DMI system by the application.

5. **277STAT** is a variation on the ASC X12 277 transaction which is used to notify the VA medical stations as to the various actions and acceptability/status of the claims. These are delivered to the medical centers via MailMan, after being processed into the DMI system by the application.

6. **Financial** applications support the processing of vendor invoices, purchase orders, payments, purchase order changes, billing documents, payment vouchers, electronic fund transfers (EFT).

d. Data is transferred between these internal systems and external systems: Veteran’s Health Administration (VHA) file servers, Veteran’s Benefits Administrations (VBA) servers, PNC Bank, Veterans Health Information Systems and Technology Architecture (VistA), and Healthcare Clearinghouses, using multiple VA approved communications protocols such as Virtual Private Networks VPN (VPNS), Mailman, and Secure File Transfer Protocol (SFTP).

**3.3.6 VA TRUSTEDLINK ENTERPRISE (TLE)**

The following provides overview information about the VA TrustedLink Enterprise (TLE) EDI environment:

a. Is comprised of TLE version 16.3.0.0 software, which is installed on a Windows 2019 server with three accompanying client interfaces (Catalyst Map, Mapping Workbench & Operations Center).

c. TLE, in combination with a COTS Business-to-Business (B2B) communications portal (Cleo VL Trader), is used and will be used to replace some current EDI translations and communications methods.

Currently, TLE is used to process healthcare claims and financial transactions and perform data extracts, transformation or translation, and load (ETL) processes.

**3.3.7 AITC BUSINESSWARE ENVIRONMENT**

The following provides overview information about the Vitria BusinessWare environment:

a. The Vitria BusinessWare environment is being migrated to Vitria

BusinessWare version 4.8 (64-bit), AITC deployments are on Red Hat Enterprise Linux (RHEL) version 7 and are being migrated to RHEL-8.

The following are applications maintained by the FTS:

1. e-Insurance Verification (e-IV) application automates the discovery of health care insurance for those Veterans VA has no record of having insurance and determines the eligibility for claimed insurance. The FSC receives HL7 transactions from the VA medical centers. The FSC determines if the Veteran’s insurance is already on file with the FSC database. If the Veteran is not in the file, the application creates an ASC X12 270 transaction which is sent to the clearinghouse for processing to the payer. The payer’s response, an ASC X12 271 transaction, is transmitted through the clearinghouse to the FSC for translation to the medical center and updating of the FSC database.

2. e-Pharmacy application enables the VA to submit pharmacy claims electronically. VA pharmacies send pharmacy claims in NCPDP format wrapped on an HL7 transaction to the FSC for processing. The FSC unwraps the claims from their HL7 wrapper and send the NCPDP transaction to the clearinghouse for processing to the payers. The corresponding adjudication results are received by the FSC from the clearinghouse, wrapped and forwarded to the medical centers.

**3.3.8 VA FSC VITRIA BUSINESSWARE ENVIRONMENT:**

a. Comprised of Vitria version 4.7 (32-bit), installed on Windows 2019.

b. The following applications are hosted and maintained by FTS:

1. The Identity Management (IdM) Service provides the capability to search for a person’s unique identity across the VA organization. Within the current scope, the ECD IdM service utilizes the centrally managed IdM Service to fulfill person search requests based on their localized identity information or trait data. For all successful search requests, the service returns the matched person’s Integration Control Number (ICN) and other available data, in synchronous fashion. Otherwise, the service will return an exception with details.

2. The Identity Management (IdM) Subscription service provides the ability to receive automatic updates from the Master Veteran Index (MVI), Identity Management (IdM) system. The IdM Subscription service routes these updates to the end user application. The Veterans’ information in the end user application is updated when MVI makes changes to Veteran’s information.

3. The CPRS Service enables Purchased Care Non-VA Care (Fee Basis) Program consults entered into Veterans Health Information Systems and Technology Architectures (VistAs) Computerized Patient Record System (CPRS) consult package to be translated and routed to the Healthcare Claims Processing System (HCPS) which generates authorizations for care. When these consults are updated or cancelled in CPRS the changes are reflected in HCPS.

4. The Camp Lejeune Family Member (CLFM) Eligibility system allows medical providers to electronically verify medical benefit coverage for the CLFM program. Medical providers can submit an electronical request and receive member benefit information in real-time allowing medical services for CLFM patients.

**3.3.9 EC/EDI PLATFORM UPGRADE**

FSC will be migrating the above EC/EDI platforms to a solution based on MuleSoft software. The project to complete this migration is expected to complete by 2024.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The PoP shall be a12-month base period with four 12-month option periods.

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

There are eleven (11) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, five are set by date:

New Year's Day January 1

Juneteenth June 19

Independence Day July 4

Veterans Day November 11

Christmas Day December 25

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

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

Martin Luther King's Birthday Third Monday in January

Washington's Birthday Third Monday in February

Memorial Day Last Monday in May

Labor Day First Monday in September

Columbus Day Second Monday in October

Thanksgiving Fourth Thursday in November

## PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities, specifically, the VA FSC facilities located at the main FSC office at 7600 Metropolis Drive, Building 5, Austin, TX and other local satellite offices within Austin, Texas. During performance of this effort, work may also be performed at the following locations:

|  |  |
| --- | --- |
| Location Name | Address |
| PITC | 5000 Wissahickon Ave  Philadelphia, PA 19144 |
| AITC | 1615 Woodward Street  Austin, Texas 78741 |
| VA Central Offices | 810 Vermont Avenue NW  Washington, DC 20420 |
| Debt Management Center (DMC) | 1 Veterans Drive  Minneapolis, MN 55417 |
| Security Investigation Center (SIC) and the Law Enforcement Training Center (LETC) | 2200 Fort Roots Drive, Building 65  North Little Rock, AR 72114 |
| VA Records Center and Vault (VARCV) | 11693 Lime Kiln Drive,  Neosho, MO 64850 |

Additional locations may be required throughout performance of this effort as VA FSC increases its customer portfolio.

Contractor employees may work off site on a case-by-case basis, with the approval of the COR and/or CO. The Contractor shall be within a commuting radius (50 miles) of the required duty station listed in the PWS placed under the terms of the task order. There shall be no additional cost to the Government for remote workers in terms of travel or labor rates.

When off-site work is permitted by the COR, the Contractor shall utilize the Government Furnished Equipment (GFE). The COR reserves the right to revoke the ability to telework as applicable.

## TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP.

The total estimated number of trips in support of the program related meetings for this effort is 88.  Anticipated locations include the following, estimated at 1-5 days in duration:

1. PITC support:

Secondary Location and Continuity of Operations (COOP) site: Austin FSC staff may be required to travel to the PITC facility, located at the address above.

1. Conferences:

To support activities under this effort, the Contractor may be required to attend the below conferences. Activities to be performed by the Contractor at these events shall include immersive hands-on training, workshops, roundtables, strategies to address the key priorities VA is working on, and an opportunity to connect with other IT leaders to provide VA with the most up to date technical information and support related to systems and services provided by VA FSC. These conferences shall only be attended with prior approval by the VA COR. The Contractor shall provide a Trip Report in accordance with PWS Paragraph 5.1.9.

a. Accredited Standards Committee’s x12 conference on conducting site visits: three times per year for at least two persons for four days per trip. x12 conference locations change annually and are announced prior to conference registration.

b. MuleSoft Conferences – 2 per year for 2 people for five days per trip

c. Plexis Conference: one time per year for two people for five days per trip. Plexis conference locations change annually and are announced prior to conference registration.

d. Pegaworld Conference: one time per year for two people for five days per trip. Pegaworld conference locations change annually and are announced prior to conference registration.

e. Gartner Conferences: 2 per year for 2 people for five days per trip. Gartner conference’s locations change annually and are announced prior to conference registration.

f. Healthcare Information and Management Systems Society (HIMSS) Conference: one time per year for two people for five days per trip. HIMSS conference locations change annually and are announced prior to conference registration.

g. Red Hat Conferences: 2 per year for 2 people for five days per trip. Red Hat conference locations change annually and are announced prior to conference registration.

h. Additional EDI Conferences: three times per year for two people for four days per trip. EDI conference locations change annually and are announced prior to conference registration.

The Government estimates that additional travel may be required, from time to time, to other remote locations/efforts listed above. The Contractor shall request and receive approval for these trips from the COR prior to travel.

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.

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

## PROGRAM MANAGEMENT

The Contractor shall provide a single point of contact for the VA COR and FSC FTS management. The Contractor shall manage the tasks, schedules, and analyze work discrepancies, communicate policies, purposes, and goals of the organization for all projects. The Contractor shall assist in analyzing and resolving programmatic issues, facilitate information exchange, and enhance management coordination between the COR/VA PM(s). This support shall include managing on-site and off-site support, any tracking of resources across projects, transitioning and onboarding of new support required, and scheduling staff to ensure support services are providing during the FSC operational hours. The Contractor shall identify point(s) of contact for all tasks under this PWS. The Contractor shall:

1. Conduct Weekly Project Progress Reviews (PPR).

2. Provide Monthly Management Reports.

3. Track deliverables across projects.

4. Coordinate, escalate and resolve project issues (e.g. risk, resources, scheduling).

5. Attend status meetings and provide status reports to project stakeholders with COR coordination.

6. Track contractor support across projects on a daily basis during normal working hours.

7. Provide a document management system, e.g. SharePoint, to track project deliverables to avoid reliance on the transmission of large files via email.

8. Track that all Contractor support:

a. Follow all documented processes and procedures utilized by VA FSC.

b. Meet all service level agreements (SLA), response and call back timeframes such as for responding to system failures and metrics in Section 6.1 of the PWS.

c. Report all hours worked into VA FSC’s Time Reporting Application on a daily basis.

d. Meet all task schedules including non-standard work schedule(s) as required. Schedules include; nights, weekends, and holidays in accordance with VA FSC requirements a non-standard work schedule, if required. Work may be required beyond normal duty hours, including nights, weekends, and holidays as necessary.

e. Comply with all VA FSC policies and processes including ProPath when applicable.

f. Comply with and support all Federal, VA and local security regulations and policies, security regulations and policies.

g. Track performance against the PWS requirements and metric.

h. Follow established change order processes.

**Deliverable:**

A. Monthly Management Reports

### TRANSITION-IN SUPPORT

The existing TO for the FSC IT support services expires on July 31, 2024. Since interruptions or delays to the work will adversely impact the mission, it is essential that attention be given to minimizing the interruption. Upon award of this effort, the Contractor shall ensure a smooth transition with the incumbent Contractor for any work requirements that are in progress at the time the incumbent TO expires. This includes providing an orderly transition of work acceptance and accomplishment so that impact to VA-FSC IT services is minimal. It also includes providing for maximum cooperation with the incumbent while ensuring that no work receives inadequate attention at the onset of this TO.

The Contractor shall plan for the transition of work to ensure continuity of services during the transition of the work from the existing contract to this TO. The Contractor shall provide a Transition-In Plan that documents the process the Contractor shall use to coordinate with the incumbent Contractor for all activities related to transition from one Contractor to another. The Contractor shall ensure link(s) to FSC SharePoint site or shared folder location where all documentation related to the contract support is stored. Additionally, the Contractor shall provide a list of meetings that require Contractor participation and the role of the Contractor staff on each meeting.

**Deliverable:**

A. Transition-In Plan

### CONTRACTOR PROJECT MANAGEMENT PLAN

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

**Deliverable**:

1. Contractor Project Management Plan

### REPORTING REQUIREMENTS

The Contractor shall provide a Weekly Division Status Report in electronic form in Microsoft Word and Project formats that describes those activities or efforts the Contractor performed for each division. The report shall include detailed instructions/explanations for each required data element, to ensure that data is accurate and consistent. The report shall identify status for each project/assignment in the division following a template to be provided by FSC. Specific projects will require additional information per management priorities as identified by the COR. The Contractor shall include a summary of each Weekly Division Status Report for the month in the monthly update to the CPMP. The Contractor shall also provide timely, ad-hoc reporting support for FSC, Congressional, or VA-Leadership through Ad-Hoc Reports, which will be defined and identified by the COR. These reports shall reflect data as of the last day of the preceding week.

The Contractor shall provide Weekly Progress Reports that cover all work completed during the reporting period and work planned for the subsequent reporting period.  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 Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the 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.

**Deliverable:**

1. Weekly Division Status Report
2. Weekly Progress Report

### 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 to the CO 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 VA FSC FTS Support 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 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.

### CONTRACTOR PERSONNEL REQUIREMENTS

Contractor personnel shall maintain a work schedule that coincides with the schedule of the VA-FSC organizations that they support. Contractor personnel shall provide services on normal Federal Government workdays during the core hours of 6:00 am Central Time (CT) to 6:00 pm CT. The Government may also require onsite support after core hours for activities covered under PWS Task 5.2 and its subparagraphs during the hours of 06:00 PM CST to 06:00 AM CST. The Contractor shall maintain the ability to increase support as required for surges in activity and shall maintain the ability to increase the level of support for all labor categories. The Contractor shall provide and continuously update a Contractor Staff Roster over the life of the TO. Contractor services at VA-FSC sites shall not occur on Federal holidays or weekends, unless authorized in advance by the COR. In general, Contractor duties shall be performed during normal business hours. However, when necessary, Contractor personnel may be required to provide services outside the normal hours of duty. These occasions will be infrequent and will require services to be performed after normal working hours, evenings, weekends (Saturday and Sunday) and/or holidays. The COR and the Contractor will mutually agree upon all deviations to the normal work schedule.

**Deliverable:**

1. Contractor Staff Roster

### TRAINING

The Contractor shall submit 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”.

Additional future training classes may be required, which will be identified by the COR. The Contractor shall ensure completion of these classes for itself and its subcontractors. Any person who does not complete required VA training will not be granted access to VA information, VA information systems, or the VA network.

Contractors who have completed these VA training courses within the past 12 months and have furnished certificates will not be required to re-take the training courses.

**Deliverables:**

A. VA Privacy and Information Security Awareness and Rules of Behavior Training Certificate/Signed Contractor Rules of Behavior/VA HIPAA Certificate of Completion

### FACILITY REQUIREMENTS

#### PHYSICAL SECURITY REQUIREMENTS

The VA-FSC is a high-security Government facility. For purposes of this specification section, “FSC”, “VA-FSC”, “premises”, “site,” “Center,” and “facility” shall mean the FSC building, any satellite offices or Philadelphia and surrounding property, including parking areas.

All Contractor and subcontractor personnel shall read and abide by the security requirements in place at this facility. Failure to comply with these security requirements may result in revocation of physical and/or electronic access privileges.

Failure to complete the work in a timely manner, or by any required completion date, caused by delays in requesting security clearances, or due to revocation of access privileges resulting solely from the actions of the Contractor or their personnel, shall not serve as the basis for an extension in task order time or cost.

The Contractor, or any subcontractors performing work on this project, shall not take any photographs on, of, or within any area of the FSC, Philadelphia or satellite locations or personnel thereon. Further, the Contractor shall not use or allow to be used any aspect of this task order for publicity or advertising purposes without specific written approval of both the FSC’s Chief of Security Services and the Contracting Officer.

Parking is provided on a “first-come, first-served” and “space available” basis. Parking is not allowed in any other location, nor is it allowed alongside the building, loading docks, or alleyways without the approval of the Physical Security Officer. Vehicles parked illegally or improperly will be ticketed or towed at the operator’s expense.

The FSC reserves the right to close the job site and order Contractor personnel off the site in the event of an emergency, Government shutdown, times of elevated security risk, or any other reason deemed necessary by FSC management or security staff. Contractor personnel must immediately leave the site and may not return until authorized by the FSC.

Security Violations: The FSC has a three-violation limit policy regarding Contractors committing security violations. The FSC is not required to provide the Contractor with any documentation related to any security violations committed by their personnel to implement any of the actions listed below:

First occurrence: A verbal warning may be given by an FSC security guard, COR, and/or Physical Security Officer.

Second occurrence: For the second occurrence of the same (or similar) violation by the same person, the person’s badge may be confiscated (by an FSC security guard, the Physical Security Officer or the Chief, Security Services); if so, the person must immediately leave the site and the person will be denied access until 7:00 a.m. the next business day.

Third occurrence: For the third occurrence of the same (or similar) violation by the same person, the person’s badge may be confiscated (by an FSC security guard, the Physical Security Officer or the Chief, Security Services); if so, the person must immediately leave the site and the person will not be allowed to access the site again.

Multiple violations and/or intentional disregard for security regulations: Any person deemed by the CO or Physical Security Officer to intentionally disregard FSC security regulations shall have his / her badge confiscated and must immediately leave the site. Future access shall be at the discretion of the CO and Physical Security Officer.

#### FSC ACCESS PRIVILEGES

Access into the FSC is only allowed through the main (south-west) entrance. The loading dock may be used to load and unload materials only (not to gain access in and out of the FSC), and only during the hours it is open (Monday – Friday, 8:00 AM to 4:00 PM CST excluding official Government holidays). If the Contractor desires to open any normally closed secure doors (or make any opening into the building structure), then it is the Contractor’s responsibility to request additional armed security officer services (using a form provided by the FSC’s Physical Security Officer) to guard the door and control access, allowing entry only by authorized Contractor and Government personnel. Contractor will be responsible for any additional cost or expenses. All personnel entering through this normally closed opening shall be screened by the security officer using a handheld metal detector. All items will be manually inspected (this includes opening and inspecting all packages) prior to being allowed entry.

If additional security officer services are required, this service shall be requested at least 48 hours in advance of when a security officer is needed. Such services shall be provided only by the FSC’s approved armed security officer services provider. Other security methods proposed by the Contractor (such as temporary walls) may be reviewed and approved, modified, or disapproved by FSC. The determination as to whether what the Contractor proposes meets the necessary level of security shall be determined by the FSC’s Chief, Security Services.

Access Cards/Badges. After award of the task order, all Contractor employees requiring long-term access (more frequent than once per month) to the FSC, or the project site may be required to obtain an FSC-issued access badge. Each Contractor or subcontractor employee shall conspicuously display, on his/her person, a Government-provided identification badge. The identification badge record and associated data will be kept in a Government-maintained computer database for security purposes.

Physical Access. Each person requiring unescorted physical access to the property will be required to submit personal identifying information (full legal name (first, middle, and last), date of birth, state-issued driver’s license or identification card number and the state that issued it, and name as it appears on the identification card. This information will be used to perform a criminal history check. Visitors who are not subjected to the criminal history check must be escorted at all times by someone who has been issued a permanent FSC ID badge. The cost of conducting the criminal history check is the responsibility of the FSC. The cost, if any, of arranging for an escort is the responsibility of the Contractor. The Contractor shall pre-screen all personnel requiring physical access to the property to ensure they are legally able to work in the U.S. and are not currently sought by law enforcement authorities.

Adjudication of information discovered during or after the criminal history check is solely the responsibility of the Chief, Security Services. Being admitted entry into the FSC based on a finding of no criminal history does not convey any security clearance. The Chief, Security Services may revoke physical access privileges at any time if criminal history is discovered, or if the person commits security incidents warranting such revocation.

#### EMERGENCY SERVICE

When an IT emergency occurs at times other than normal business hours, the Contractor shall respond no later than (NLT) one (1) hour after notification of the emergency issue. The Contractor shall prepare and submit a written IT Emergency Resolution Report within two (2) business days after the emergency has been resolved. The report shall include the date and time of the service call, the actions performed, the name of the technician(s) working on the issue, and when normal IT operations were restored. The Contractor shall respond to callbacks and serve as the initial point of contact for system failures. The Contractor shall be available by Contractor-provided cell phone or pager, which will be used by the Government to contact the Contractor for callback purposes. An “emergency” is defined as a situation or act that impacts the services the FSC provides to its customers.

**Deliverable:**

A. IT Emergency Resolution Report

### PROFESSIONAL STANDARDS REQUIREMENTS

The Contractor shall be responsible to ensure its personnel providing services have the appropriate qualifications for the TO. Contractor personnel shall perform the services in a professional manner. Contractor personnel will be denied access to VA-FSC facilities if such action is determined to be in the best interests of VA by the CO. Examples of reasons the CO may deny access to the VA-FSC facility include Contractor employees violating the law, VA security or confidentiality requirements, and/or for other violations of facility policies.

Contractor personnel performing on-site at VA-FSC facilities shall:

1.) Adhere to VA-FSC IT staff policies. This includes, but is not limited to the following:

A. Comply with VA-FSC configuration management and network security policies.

B. Follow VA-FSC Change Advisory Board (CAB) procedures.

C. Communicate recommendations orally and in writing to higher organizational management.

D. Ensure changes made while performing technical services shall be documented in writing and made available to the VA-FSC IT staff.

E. Attend required meetings and conferences.

F. Exemplify professionalism in the areas of timeliness, communication, analytical techniques, confidentiality, cooperation, and demeanor.

G. Maintain daily time in the VA FSC designated time tracking system.

2.) Adhere to the same professional and ethical standards of conduct required of Government personnel. The Contractor shall not:

A. Discuss with unauthorized persons any information obtained in the performance of work under this task order;

B. Conduct business not directly related to this task order on VA-FSC premises;

C. Use computer systems and/or other VA-FSC facilities for company or personal business; or

D. Recruit on VA-FSC premises or otherwise act to disrupt official Government business.

The Contractor shall safeguard all sensitive information and use the information exclusively in the performance of this TO. The Contractor shall follow all Government rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations. The Contractor shall limit access to the minimum number of Contractor employees necessary for task order performance for all information considered sensitive in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the TO, the Contractor has a responsibility to ask the COR or other Government's representative for clarification. The Contractor shall indoctrinate all personnel employed by the Contractor and any Subcontractors involved in this task order on their roles and responsibilities for proper handling and nondisclosure of sensitive information. The Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information.

The Contractor shall not use any offshore resources (e.g. personnel, hardware, software) in support of the services being provided under this TO. Data used on this TO shall not be transmitted to or stored at an offshore location. For the purposes of TO, offshore is defined as being any location outside the United States, its possessions, and Puerto Rico.

### TRIP REPORTING

The Contractor shall travel at the request of FSC to attend program-related meetings or conferences throughout the period of performance.  Contractor employees may be required to travel for the purpose of attending remote training sessions, performing a site visit to a VA-FSC customer, performing work at the FSC’s back-up facility in Philadelphia, or attending professional conferences. At the conclusion of each trip, the Contractor shall submit a Trip Report detailing trip activities and items of relevance to FSC current and future operations.

**Deliverable**:

A. Trip Report

### ACTIVITY-BASED COSTING LABOR TRACKING

The Contractor shall input their work hours by activity into the VA-FSC’s Activity-Based Costing (ABC) Labor Tracking system each Government Pay Period. ABC Labor Tracking system is used as a driver quantity to assign resource cost to activities and activity cost to products and services within the organization. The quantities from ABC Labor Tracking system makes activity cost visible throughout the organization, incentivizes cost reduction, increases precision of overhead allocation, and enables informed pricing decisions.

The Contractor shall complete the input of hours into the ABC Labor Tracking system no later than the first Monday of the Government Pay Period.

## FTS OPERATIONS AND MAINTENANCE SUPPORT

The Contractor shall include a summary of all Operations and Maintenance activity in the monthly update to the CPMP. The Contractor shall support FSC operations at all current locations, future locations, and virtual employees. The Contractor shall provide recommendations to improve the FSC complete infrastructure, and address/lead critical issues and root cause analysis. The Contractor shall assist in helping FSC FTS support the FSC business objectives to meet these goals with technology. In addition, the Contractor team shall be required to balance team-working skills and the ability to work alone as well as quickly assimilate and communicate technical and non-technical information. In all aspects of support to FTS, the Contractor shall participate in meetings and activities that support software projects, software maintenance releases, and emergency software releases. This support shall include architecture support, database, security scanning/ testing, providing operational assistance to software deployment and providing documentation deliverables that align with VIP.

### TECHNICAL WRITING

The Contractor shall create high quality documents which will be used by both technical and non-technical personnel across all departments in FTS. The Contractor shall:

a.) Develop written information about the organization’s computing systems that aid in their development, use, and support.

b.) Liaise with department heads and end users to identify and document business procedures and establish documentation needs for all FSC IT infrastructure including hardware and software.

c.) Liaise with printers and graphic artists to plan layout, graphical elements, and formatting of documents. Ensure final documents are usable and of high quality. Research, evaluate, and recommend new documentation tools and methods in support of documentation improvement efforts.

d.) Establish, communicate, and maintain documentation, and provide training where required.

The Contractor shall support system sustainment documentation activities including:

a.) Edit written documentation of development and other IT staff to create unified and consistent support documents.

b.) Revise all documentation to incorporate system changes and other updates.

c.) Create and maintain documentation (process workflows, standard operating procedures, user guides, data dictionaries, etc.).

d.) Gather information by observing developmental and production activities, by studying product plans, drawings, specifications, and samples and by interviewing production, development, and engineering personnel to become familiar with product technologies, uses, operation, and maintenance.

e.) Create/update documentation as necessary in accordance with all requests for change (RFC).

f.) Manage and maintain administrative documentation.

g.) Produce status reports for internal and external customers as needed.

h.) Support documentation needs as part of the Assessment & Authorization (A&A) process, Systems and Applications scans and audits, and any other activity requiring creation and/or modification of systems and applications documentation.

The Contractor shall support VIP documentation activities including:

a.) Analyze IT project requirements to determine types of documents needed. Collaborate with sustainment and development staff to collect and interpret technical information.

b.) Plan, design, research, write, and edit a range of documents, including user guides and manuals, technical specifications, training materials, user policies, and proposals, sustainment support for both print and online media.

c.) Maintain online archives of project documentation.

d.) Assist other team members in creating and reviewing VIP compliant documentation.

### DISASTER RECOVERY ANALYSIS AND SUPPORT

Continuity of operations includes, but is not limited to, disaster recovery and IT contingency. The Contractor shall maintain a Disaster Recovery Plan (DRP) and Information Systems Contingency Plans (ISCP), and support Continuity of Operations Plans (COOP) by compiling all Contingency planning, procedures, and documentation from the following PWS Tasks, which include, but are not limited to:

(a) Systems Administration; (b) Network Administration; (c) Database Administration; (d) Privacy Services; (e) IT Service Desk; (f) Application Production Support and Maintenance; (g) Enterprise Content Management and Application Administration Services; (h) Scanning Support; (i) Systems Analysis Support; (j) Cloud System Engineering; (k) EDI Application Support; (l) Systems Administration; (m) Network Administration; (n) Database Administration; (o) Privacy Services; (p) IT Service Desk; (q) Application Production and Maintenance Services; (r) Enterprise Content Management Application and Administration Services; (s) Scanning Support; (t) Data Analytics Support, and (u) Systems Analysis Support.

The Contractor shall provide analysis and support for disaster recovery and continuity of operations including:

a.) Analysis of program and project disaster recovery plans and systems.

b.) Identification of areas needing improvement.

c.) Recommendation of strategies and approaches for strengthening existing or developed DRP and ISCP.

d.) Work with FSC Emergency Preparedness, Response and Continuity (EPR-C) to ensure DR and ISCPs integrate approved common Threat, Hazard Identification and Risk Assessment (THIRA) data.

e.) Work with system owners and EPR-C to develop ISCP validation procedures for restored systems.

f.) Develop and implement plans and procedures to ensure the FSC has a reliable and proven DRP and ISCP that meets the COOP BIA Maximum Tolerable Downtimes (MTD).

g.) Document any gaps between MTD and system Recovery Time Objectives (RTO) in a specific ISCP Gap Analysis annex.

h.) Perform quarterly reviews of the DR and ISCPs to ensure they are accurate and updated to meet new requirements.

h.) Document all the necessary system processes and procedures to support the DR, and ISCPs plans.

i.) Implement and execute a plan to test the DRP and ISCP, and work with EPR-C to support needed COOP capabilities.

j.) Evaluate tests of the DRP and ISCP, identify and address changes or new processes to support both plans.

k.) Compile and update all documentation for tests and exercises to include development of improvement and corrective action plans.

l.) Ensure DR and ISCP addresses all business and IT requirements related to availability and sustainment of systems and applications in case of an emergency or disaster.

### INFRASTRUCTURE SUPPORT

#### SYSTEMS ADMINISTRATION SERVICES

The Contractor shall:

a.) Design, install, and support connectivity of computer and network systems to ensure the stable operation of the organization’s IT assets. This includes developing, configuring, maintaining, supporting, and optimizing all new and existing infrastructure hardware, software, and communication links.

b.) Configure and maintain all VA-FSC computer room equipment.

c.) Administer, operate, and maintain VA-FSC servers.

d.) Proactively analyze event logs on all servers and apply corrective action when necessary.

e.) Provide preventative maintenance services and troubleshoot each physical and virtual server and any associated software or hardware to ensure all servers and associated components that comprise VA-FSC IT Infrastructure are operational 99.99% of the time. Computation excludes scheduled, pre-agreed outages and outages caused by VA provided equipment, power, cable plant, and/or user generated disruption of service.

f.) Install as required/mandated anti-virus and/or security patches and remediate all identified vulnerabilities within VA and FSC guidelines.

g.) Plan, document, and test for ISCP, COOP, which includes, but is not limited to disaster recovery and IT contingency, and create and maintain, as needed, COOP ISCP documentation which includes a hardware list, a software configuration list and a system prioritization list for when powering on systems/applications. This documentation shall be included in the COOP ISCP Plan required in Section 5.2.4.

h.) Comply with all Federal, VA and VA-FSC security, privacy, and facility policies and regulations.

i.) Participate in the Authority to Operate (ATO) assessment and accreditation process.

j.) Administer FSC user accounts and passwords in an MS Active Directory domain.

k.) Provide MS Group Policy Object (GPO) management.

l.) Provide system resource management.

m.) Administer and maintain servers with remote desktop application software and other approved administration tools.

n.) Install, configure, and administer the VA-FSC MS Internet Information Services (IIS) and associated services, such as intranet.

o.) Integrate COTS software and hardware products into the VA-FSC IT architecture.

p.) Comply with commercial licensing requirements for all VA-FSC systems.

q.) Troubleshoot server administration routines through direct command line interfaces or through alternate software programming packages.

r.) Perform day-to-day system backup and recovery operations on VA-FSC IT Infrastructure managed web, application, and database servers.

s.) Ensure proper backups of VA-FSC systems and data. Provide daily detailed reports on backup status.

t.) Manage FSC centralized storage, environments, storage networks, and any other technologies classified as a storage technology.

u.) Maintain and monitor server hardware, storage networks, and associated hardware including periodically testing backup processes to include full restoration of one or more systems.

v.) Administer the VA-FSC Cisco based local area network (LAN).

w.) Design, test, install, maintain, and document for VA-FSC computer networks at both the Austin, Texas and Philadelphia, Pennsylvania facilities.

x.) Operate and maintain solutions hosted in the VAEC in accordance with the application and VAEC SLAs.

y.) Support solution builds and release management, asset management, and change and configuration management.

z.) Support solution security assessment activities, scans, and audits to include control reviews.

aa.) Update server responsibility matrix listed in the FSC Application List

bb.) Create and update Standard Operating Procedures (SOPs) for systems/processes required to provide the services identified in this PWS.

cc.) Provide Updated Product Operations Manuals (POMs) for each system/process.

dd.) Provide a Systems Administration Weekly Status Report detailing status of servers/applications for system health and availability, and accomplishments. This shall be included as part of the Weekly Division Status Report under PWS 5.1.3

ee.) Provide a Monthly Backup Report

ff.) Provide a Monthly Storage Utilizations and Capacity Report

gg.) Install, configure, and maintain system and application monitoring and dashboards for all FSC systems, update monitoring service registry and produce Monitoring Plan

**Deliverables:**

A. System/Process SOPs

B. Updated System/Process Product Operations Manuals

C. Monthly Backup Report

D. Monthly Storage Utilizations and Capacity Report

E. Monitoring Plan

#### NETWORK ADMINISTRATION SERVICES

The Contractor shall:

a.) Provide LAN administration, including installing, configuring, and testing systems, diagnosing and troubleshooting LAN hardware and software, controlling, documenting LAN configurations.

b.) Comply with VA-FSC, VA OI&T, VA, and federal regulations, performing updates to the VA-FSC network equipment.

c.) Respond to network-related issues and requests for system service.

d.) Troubleshoot and coordinate resolution of network problems and issues.

e.) Perform configuration management for all network devices.

f.) Determine, recommend, develop and implement the most effective and efficient IT hardware, software and communication solutions for the VA-FSC IT network.

g.) Research, evaluate, recommend, develop, integrate, test, configure, monitor, and install information technology solutions, including hardware, software, communications products and services on the VA-FSC LAN.

h.) Configure, test, document test results and provide recommendations to the VA-FSC configuration control board on integrating new web-based applications into the enterprise environment.

i.) Identify security requirements and specifications; provide technical support of requests for data gathering, perform technical analyses, and document security requirements; conduct studies and prepare evaluations regarding the feasibility of using new technology.

j.) Implement and maintain network security countermeasures, boundary protection and Network Intrusion Detection.

k.) Configure Public Key Infrastructure (PKI) enabled web applications on the VA-FSC network.

l.) Provide preventative maintenance services and troubleshoot each Local Area Network (LAN) and Storage Area Network (SAN) physical and virtual component and any associated software or hardware to ensure all LAN components that comprise VA-FSC IT Infrastructure are operational 99.99% of the time. Computation excludes scheduled, pre-agreed outages and outages caused by VA provided equipment, power, cable plant, and/or user generated disruption of service.

m.) Provide Network Diagrams including LAN/WAN, rack elevation, and connectivity.

n.) Support planning, documentation, test, and execution for all DRP/ISCP-related activities, and create and maintain, as needed, Network ISCP Documentation which includes a hardware/software list and configurations and a system startup prioritization. This documentation shall be included in the ISCP described in Section 5.2.4.

o.) Create and update Network SOPs.

p.) Provide POM updates.

q.) Provide a Network Administration Status Report detailing status of servers/applications for system health and availability, and accomplishments. This shall be reported under the Weekly Division Status Report under PWS 5.1.3.

r.) Provide rapid and accurate changes to the network in support of evolving business and operational needs to include network automation, practice of monitoring, managing, automating, and operating a network/software defined network.

**Deliverables:**

A. Network Diagrams

B. Network SOPs

#### DATABASE ADMINISTRATION SERVICES

The Contractor shall:

a.) Support, evaluate, review, and manage database resources and services across the organization to preserve high levels of data quality and integrity.

b.) Assist in the development, implementation, and enforcement of database policies and procedures to ensure the integrity and availability of databases and their accompanying software.

c.) Administer and maintain instances of MS SQL 2016/2019 (or current) and Oracle 19c (or current) database servers consisting of over 1500 individual databases.

d.) Administer and monitor all redundancy SQL and Oracle database server implementations; services including database mirroring, clustering, replication, or any similar database fail-safe implementations.

e.) Design, create, integrate, test, implement, maintain and manage VA-FSC databases using MS SQL server, Oracle database technologies, SharePoint Portal Server, and others when required.

f.) Monitor the daily performance of all databases to include growth of all databases/platforms, anticipate and plan for change, growth, and expansion.

g.) Install as required/mandated all required security updates, patches and components with COR approval.

h.) Provide support for the COOP, through planning, documentation testing, and execution for all COOPISCP-related activities, which includes, but is not limited to disaster recovery and IT contingency, and create and maintain, as needed, COOP ISCP documentation which includes a hardware/software list and configurations and system startup prioritization. This documentation shall be included in the COOP ISCP Plan required in Section 5.2.4.

i.) Comply with all Federal, VA and VA-FSC security, privacy, and facility policies and regulations.

j.) Participate in the ATO assessment and accreditation process.

k.) Monitor and tune application SQL and Oracle query performance for production applications.

l.) Review application queries and stored procedures for security-related vulnerabilities.

m.) Perform analysis of SQL and Oracle-based applications.

n.) Administer VA-FSC policies and procedures to control movement or migration of new and revised databases and applications to a production environment.

o.) Investigate new SQL Server and Oracle database technologies and tools for possible integration into VA-FSC operations.

p.) Develop and implement database-related Service Requests.

q.) Create new and maintain current report jobs and procedures.

r.) Establish libraries of scripts and stored procedures to assist developers and improve code reuse.

s.) Establish and maintain user access control appropriate to each database environment consistent with VA-FSC security policy.

t.) Monitor and administer user access, authentication, Single Sign on, logins and passwords for all FSC databases.

u.) Perform database upgrades in conjunction with the administrator of the operating system.

v.) Build and configure new SQL Server and Oracle Database platforms when required.

w.) Ensure production databases are available to VA-FSC users and customers in support of FSC timeframes.

x.) Perform day-to-day database backup and recovery operations.

y.) Ensure daily, weekly, and monthly production jobs against all FSC databases execute.

z.) Periodically test database backups and tapes, to include full restoration of one or more databases or entire database server.

aa.) Monitor all FSC databases for security breaches; investigate or support investigation of possible breaches with security personnel.

bb.) Maintain a platform test environment and other necessary environments to test the impact of database upgrades and patches prior to installation; perform tests of upgrades/patches before moving or migrating to production; plan the move of patches to production.

cc.) Research and integrate COTS software and hardware products with FSC databases.

dd.) Develop, monitor, and administer VA-FSC databases.

ee.) Interface with application/database developers to design and implement new databases and/or design changes; develop physical schema designs.

ff.) Manage database data-level encryption, encrypted data security access to authorized applications and individuals.

gg.) Review, monitor, set-up, or perform restart and database recovery procedures to include data, log, and transaction recoveries.

hh.) Integrate and maintain heterogeneous, multi-vendor software and database applications as required to support FSC application and enterprise systems.

ii.) Ensure data structures are designed to support linkages.

jj.) Ensure test recovery procedures for databases and for web and application servers are accurate, and written recovery procedures tested twice a year.

kk.) Provide and assist with troubleshooting all application and enterprise system errors originating from or involving a component of the FSC Database environments.

ll.) Test and install new releases/versions/fixes of all database-related software on specified platforms.

mm.) Respond to callback and serve as the initial point of contact for failures of the FSC database enterprise components and products and ensure and coordinate the resolution and correction of failures.

nn.) Implement approved customer requests for changes to the databases.

oo.) Respond to VA-FSC Help Desk tickets within specified time periods as defined by VA OI&T standards for IT Help Desk.

pp.) Respond to database problems in all environments: production, preproduction, test, User Acceptance Test, and development.

qq.) Configure and maintain all essential security controls and Security Technical Implementation Guides (STIGS) on all database environments.

rr.) Provide preventative maintenance services and troubleshoot each database instance to ensure database components that comprise VA-FSC IT Infrastructure are operational 99.99% of the time. Computation excludes scheduled, pre-agreed outages and outages caused by VA provided equipment, power, cable plant, and/or user generated disruption of service.

ss.) Provide Data Dictionaries including maintaining the table, data elements, domains, and views for FSC databases.

tt.) Update Database Administration SOP

uu.) Provide POM updates.

vv.) Provide Database Administration Status detailing status of databases, database backups, database redo logs, and database team accomplishments. This shall be reported under the Weekly Division Status Report under PWS 5.1.3

**Deliverables:**

A. Data Dictionaries

#### CYBERSECURITY

The Contractor shall:

a.) Provide continuous monitoring of FSC network, systems, applications, databases, and IT infrastructure.

b.) Maintain an enterprise vulnerability management program. Perform vulnerability scanning support and provide recommendations to IT Technicians to fix and/or remediate security vulnerabilities.

c.) Develop and recommend technical solutions to support client/customer requirements in solving moderately and highly complex network, platform, and system security problems. Typical focus areas include analytical and engineering solutions based on federal and industry Information Security (INFOSEC) policy, doctrine, and regulations.

d.) Provide support for identity management, secure system engineering and development, biometrics, system/security requirements analysis, and secure system definition.

e.) Support specification development and implementation of INFOSEC policies and procedures utilizing technical and analytical skills.

f.) Design test beds for the Developmental Test & Evaluation (DT&E) of advanced INFOSEC hardware and software solutions.

g.) Perform penetration tests of FSC infrastructure and applications to attempt to penetrate FSC network and/or computer systems for the purpose of finding and fixing computer security vulnerabilities. This support shall be required for all software development efforts. Document and provide a Penetration Test Result Report.

h.) Ensure that all vulnerabilities and associated data calls are completed 99.99% within the specified timeliness.

i.) Develop and maintain SOPs and playbooks.

j.) Assist in the design and implementation of secure software development practices.

k.) Ensure secure application deployment and configuration in accordance with VA application security policies and standards.

l.) Collaborate with other teams to ensure secure application deployment and configuration.

n.) Collaborate with Blue Team to enhance organization's overall security posture.

o.) Conduct proactive research to identify potential future threats, vulnerabilities, and mitigation techniques.

1. Conduct ongoing analysis of security trends and emerging threats to enhance detection capabilities.

q.) Collaborate with other teams to provide actionable threat intelligence and recommendations.

**5.2.4.4.1** **Web Application Security Assessment (WASA)**

1. Conduct secure code reviews and identify vulnerabilities in web applications.
2. Complete annual web application security assessment and assessment report; share results with Business Owners and validate remediations in accordance with VA SOPs
3. Conduct penetration testing and produce Penetration Test Result Report on all applications.
4. Support development and enforce application security policies and standards.
5. Provide training and guidance on secure web application coding practices to development teams.
6. Conduct proactive research to identify potential future threats, vulnerabilities, and mitigation techniques.
7. Participate in information sharing and collaboration with external threat intelligence organizations.
8. Conduct offensive security testing to identify vulnerabilities and weaknesses.
9. Identify and recommend mitigation strategies for identified vulnerabilities; research and assess emerging security vulnerabilities and threats.

**Deliverables:**

1. Web Application Security Assessment report
2. Penetration Test Result Report

**5.2.4.4.2 Threat Intelligence & Modeling (TIM)**

1. Identify and remediate cyber threats and vulnerabilities in Application Programming Interfaces (APIs), connections, system, and end-to-end networking devices.
2. Collect and analyze information on emerging threats and attack vectors.
3. Identify and track threat actors and their tactics, techniques, and procedures (TTPs)
4. Monitor and analyze open-source intelligence (OSINT) for relevant cybersecurity information.
5. Maintain and update threat intelligence platforms and tools.
6. Participate in information sharing and collaboration with external threat intelligence organizations.
7. Provide post-incident analysis and recommendations for improving security controls.
8. Conduct offensive security testing on APIs, systems, and devices to identify vulnerabilities and weaknesses.
9. Perform social engineering and phishing attacks to test organization's defenses.
10. Create and execute simulated cyber-attacks to measure response capabilities.
11. Identify and recommend mitigation strategies for identified vulnerabilities.
12. Develop and maintain attack scenarios and playbooks.
13. Produce quarterly System Threat Intelligence and Assessment reports to evaluate vulnerabilities, threats, and gaps on system connections.
14. Conduct daily assessments on call centers to assess compliance with VA policies and procedures; provide Daily Call Center Failure Reports.
15. Produce Monthly Secret Shopper Report that consolidates findings, trends, and recommendations based on Daily Call Center Failure Reports.

**Deliverables:**

1. Quarterly System Threat Intelligence Assessment Reports
2. Daily Call Center Failure Reports
3. Monthly Secret Shopper Report

**5.2.4.4.3 Internal Security Monitoring & Alerting (ISMA)**

1. Conduct regular security monitoring and analysis of network and system logs.
2. Manage and operate security monitoring tools, SIEM (Security Information and Event Management) systems, and other security technologies.
3. Monitor, investigate, and respond to security alerts and incidents.
4. Perform incident triage and escalate high-priority incidents to appropriate teams.
5. Coordinate with external incident response resources.
6. Identify and track threat actors and their tactics, techniques, and procedures (TTPs).
7. Collaborate with other teams to provide actionable intelligence and recommendations.
8. Participate in information sharing and collaboration with external threat intelligence organizations.
9. Monitor, detect, and respond to security incidents in real-time.
10. Conduct root cause analysis to identify the source of security incidents.
11. Provide post-incident analysis and recommendations for improving security controls.
12. Conduct weekly assessment of inactive devices on the FSC’s network; produce Weekly 90 Day Inactivity Laptop List
13. Suspend accounts associated with devices that have been inactive for 90 days or more.
14. Conduct weekly Nessus scans on the environment; conduct Weekly FSC Scan Analysis to ensure remediations are being addressed.

**Deliverables:**

1. Weekly 90 Day Inactivity Laptop List
2. Weekly FSC Scan Analysis

**5.2.4.4.4 INFORMATION ASSURANCE**

The Contractor shall provide support for the Assessment and Authorization (A&A) process to obtain ATO certification in compliance with the most current versions of VA Handbook 6500, VA Handbook 6500.6 (Section 3), and VA Handbook 6500.3 for FSC IT systems and applications. The Contractor shall manage requirements to ensure all documents and artifacts are updated accordingly, prepare/update and maintain the A&A/ATO Documentation, ensure artifacts and documents are uploaded into the current VA Risk Management tool, and manage remediation efforts for identified ATO vulnerabilities. The Contractor shall develop and submit all required security document artifacts as described in the following link: <http://vaww.oed.wss.va.gov/process/maps/process_AAA.pdf>. The Contractor shall perform security forensics on identified compromised systems, prepare findings reports, report findings to leadership within 12 hours of finalized report, and maintain historical evidence according to VA policy and procedures. VA requires an ATO for any device connected to the production network as well as the external hosting environment.  After ATO is achieved, the Contractor shall update and maintain the A&A/ATO Documentation as required to ensure compliance.  The Contractor shall:

a. Perform bi-weekly reviews of Plan of Actions and Milestones (POA&M) with the VA PM/COR to ensure backlog is scheduled and prioritized for remediation, and to verify that defined milestones will be achieved.

b. Perform monthly reviews of Risk Based Decisions with the VA PM/COR to ensure remediation of outstanding risks or path forward is identified and achievable.

c. Support documentation of a Data Use and Reciprocal Support Agreement (DURSA)/Memorandum of Understanding (MOU)/Interconnection Support Agreement (ISA) between the hosting environment and VA, if applicable.

**Deliverable:**

A. A&A/ATO Documentation

#### IT SERVICE DESK

The Contractor shall provide IT Service Desk support including:

a.) Provide a single point of contact for end users to receive support and maintenance within the organization’s desktop computing environment. This includes installing, diagnosing, repairing, maintaining, and upgrading all PC and laptops hardware and equipment to ensure optimal workstation performance. Troubleshoot problem areas (in person, by telephone, or via e-mail or remote access tools) in a timely and accurate fashion and provide end-user assistance where required.

b.) Support the development of long-term strategies and capacity planning for meeting future desktop hardware, software, and mobile devices needs.

c.) Conduct research on desktop, laptop, and mobile devices products in support of procurement and development efforts. Evaluate and recommend products for purchase and provide a Product Evaluation Recommendation Report.

d.) Write technical specifications for purchase of PCs, laptops, mobile devices, desktop hardware and related products and provide a Product Technical Requirements Report.

e.) Perform onsite analysis, diagnosis, and resolution of complex desktop problems for end users, and recommend and implement corrective solutions, including offsite repair for remote users as needed.

f.) Install, configure, test, maintain, monitor, and troubleshoot end-user workstations, mobile devices, and related hardware and software to deliver required desktop service levels.

g.) Assess the need for and implement performance upgrades to PC boxes, laptop, and mobile devices including the installation of CPUs, I/O and NIC cards, ribbon cables, hard drives, RAM, memory chips, CD-ROMs, and other devices.

h.) Collaborate with LAN technicians/network administrators to ensure efficient operation of the desktop computing environment.

i.) Administer and resolve issues with associated end-user workstation networking software products.

j.) Perform workstation moves, adds, and changes (MAC) requests as they are submitted by management.

k.) Ensure that physical desktop connections (i.e., RJ-45 Ethernet jacks, RJ-11 telephone modem jacks, connectors between PCs and servers) are in proper working order.

l.) Prepare and conduct tests and implement applications for monitoring desktop performance and provide performance statistics and reports.

m.) Assist in preparing, maintaining, and upholding procedures for logging, reporting, and statistically monitoring desktop operations.

n.) Maintain an inventory of all IT desktop, laptop, and mobile devices, hardware such as monitors, keyboards, hard drives, modems, network cards, and other components and equipment.

o.) Provide reporting information regarding inventory of hardware and software and recommend purchases and updates when required.

p.) Accurately document instances of desktop equipment or component failure, repair, installation, and removal.

q.) Liaise with third-party support and PC equipment vendors.

r.) Operate within Microsoft Windows 10 (or current) Professional environments and future standard workstation PC, laptops, and mobile devices client configurations using the latest VA-approved web browsers as front-end interfaces.

s.) Design and implement workstation PC, laptops, and mobile devices standard configuration and images following VA OIT guidance and regulations.

t.) Test and implement new workstation PC, laptops, and mobile devices software.

u.) Perform all installs, moves, additions, patches, updates, and changes required for workstation PC, laptops, and mobile devices support, which includes MS Windows 10 (or current), device drivers, MS Office suite, MS Edge (or current) web browser, MS Outlook, anti-virus, and most other general-purpose PC software packages.

v.) Install as required/mandated anti-virus and/or security patches.

x.) Comply with all Federal, VA and VA-FSC security, privacy, and facility policies and regulations.  
 y.) Perform asset management (e.g., asset inventory, auditing and tracking, asset administration and reporting, and history and forecasting).

z.) Answer, evaluate and prioritize incoming calls, voice mail, e-mail, Instant Messaging, IT Support software (i.e., ticketing system) and in person requests for assistance from customers experiencing problems with hardware, software, networking, and other IT related technologies.

aa.) Identify when a problem requires the next level of support and elevate the problem following established procedures.

bb.) Log and track calls using problem management database or system. Maintain historical records and related problem documentation.

cc.) Repair computers, printers, and peripherals, including diagnosis of system malfunctions, development of cost estimate for repair; apply most cost-effective solution to repair system malfunctions.

dd.) Support end users in the resolution of day-to-day problems that occur when using their government furnished computer hardware or software.

ee.) Upgrade all VA provided or Government Furnished Products (GFP) computer hardware, including memory, hard drives, CD-ROM drives, DVD drives, floppy drives, VA approved thumb drives, monitors, modems, motherboards, processors, video cards, sound cards, network cards, and other special purpose cards.

ff.) Prepare standard statistical reports, such as help desk incident reports and system and enterprise status reports. Analyze and evaluate incident reports and make recommendations to reduce help line incident rate.

gg.) Perform all desktop and laptop remediation of data calls, ensure all software and components are current, patched and upgraded adhering to VA standards.

hh.) Ensure Help Desk tickets meet the following communication intervals:

a) Critical/P1: Within 30 minutes of known outage, for initial notification. Hourly updates notifications and final notifications when service restoration is confirmed.

b) High/P2: Within 30 minutes of known outage, for initial notification. Updates notifications every 2 hours and final notifications when service restoration is confirmed.

c) Moderate/P3: Within 12 hours of known outage, for initial notification. Daily update notifications and final notifications when service restoration is confirmed.

d) Low/P4: Within 24 hours of known outage, for initial notification. Update notifications every 72 hours and final notifications when service restoration is confirmed. Ensure that all Help Desk tickets are worked, completed with fully documented notes and resolution within three (3) days of receipt with 95% compliance.

ii.) Ensure Help Desk tickets meet the following target resolution time frames:

a) Critical/P1: 24 hours from escalation to Major Incident by Incident Manager to return to acceptable service

b) High/P2: 2 business days from escalation to Major Incident by Incident Manager to return to acceptable service

c) Moderate/P3: 4 business days

d) Low/P4: 10 business days

jj.) Maintain a Dashboard with reporting capabilities with information on all data calls received and their completion status.

kk.) Provide a Weekly ServiceNow Ticket Report to document volume and status of tickets generated.

**Deliverables:**

A. Product Evaluation Recommendations Report

B. Product Technical Requirements Report

C. Weekly ServiceNow Ticket Report

### APPLICATION PRODUCTION SUPPORT AND MAINTENANCE SERVICES

The Contractor shall provide Application Production Support and Maintenance for FSC’s 3rd party software applications. The Contractor shall:

a.) Support the operations end of all FSC’s systems and applications, including 3rd party software applications, and associated Web sites and keep them running smoothly.

b.) Support installation and integration of 3rd party applications with back-end services for FSC databases, FSC Enterprise Service Bus (ESB), and other existing FSC applications.

c.) Support migration of applications to the VAEC by:

i) Working with other technical staff to assess applications for cloud-hosting readiness

ii) Identifying and documenting necessary changes to enable the application to be migrated to and hosted at the VAEC

iii) Implementing application changes

iv) Testing and validating changes

v) Supporting and providing coordination and execution of application migrations to VAEC

vi) Updating all documentation impacted by the cloud migration

d.) Perform day-to-day administration of cloud-based applications.

e.) Provide application production support of FSC's 3rd party software applications.

f.) Coordinate, troubleshoot, maintain, support, patch and upgrade existing FSC 3rd party applications.

g.) Apply best practices related to application production support of mission-critical information and software systems. This includes configuration, monitoring, performance tuning and security best practices.

h.) Install as required/mandated application security patches, application updates and upgrades.

i.) Plan, document, test, and execute COOP ISCPs for FSC’s 3rd party software applications and create and maintain, as needed, COOP ISCP documentation which includes application configuration list and system prioritization list for when powering on systems/applications. This documentation shall be included in the COOP ISCP Plan required in Section 5.2.4.

j.) Plan, document, update, and manage the backup and restore process and procedures, User access and control, monitoring metrics, data flow diagrams, and POM for FSC’s 3rd party applications.

k.) Comply with all Federal, VA and VA-FSC security, privacy, and facility policies and regulations.

l.) Participate in the assessment and accreditation process for obtaining an ATO for FSC’s 3rd party applications.

m.) Create and update Application Access and Authorization Matrix for each new application; maintain and update documentation for current applications.

n.) Create and update Application SOPs

o.) Report Accomplishments as part of the Weekly Division Status Report under PWS 5.1.3

p.) Input data into a variety of different business/software systems and networks to maintain integrity of existing systems; data can be input manually or using automated financial management tools. Review entered data for completeness and accuracy.

q.) Perform data validation and pull standard and ad hoc reports.

**Deliverables:**

A. Application Access and Authorization Matrix

B. Application SOPs

### ENTERPRISE CONTENT MANAGEMENT (ECM) APPLICATION AND ADMINISTRATION SERVICES

The Contractor shall:

a.) Provide Database Administration as it relates to the ECM system.

b.) Support migration of ECM enhancements from the Development system to systems in lower environments including but not limited to Test, User Acceptance Test (UAT), Pre-Production, and Production.

c.) Support replication of ECM applications/systems from Development to other lower environments including but not limited to Test, UAT, Pre-Production, and Production system.

d.) Test and fine-tune ECM and related systems.

e.) Implement ECM application maintenance and bug fixes.

f.) Upgrade the ECM scripts to Business Process Interface (BPI).

g.) Troubleshoot ECM issues, which includes:

i) Working on issues related to VA-FSC DMS and/or IBM FileNet, which, at a minimum, includes PC workstations and laptops, servers, printers, optical jukeboxes and scanners.

ii) Providing ECM user assistance.

iii) Providing ad hoc training on all ECM application software.

iv) Responding to VA FSC ECM Help Desk tickets on scheduled response time listed on ticket.

v) Handling problem escalation of ECM and customer application issues through the Contractor Help Desk and ECM support.

vi) Comply with all Federal, VA and VA-FSC security, privacy, and facility policies and regulations.

vii) Participate in the assessment and accreditation process to maintain existing and obtain new ATOs, by providing ECM specific support documentation

viii) Incorporating into design and implementation, the production control processes that identify problems and provide prompt resolution, using Lean Six-Sigma processes improvement techniques.

h.) Provide FileNet configuration and sustainment activities in support of FSC software projects, software maintenance releases, and emergency software releases.

i.) Support ECM-related software projects with documentation deliverables. Those deliverables shall align with VIP.

j.) Participate in project meetings and activities in support of operations and maintenance activities, FSC software projects, software maintenance releases, and emergency software releases with an ECM component.

k.) Create and update ECM SOPs

l.) Provide ECM Status under the Weekly Division Status Report under PWS 5.1.3

**Deliverables:**

A. ECM SOPs

### SCANNING SUPPORT

The Contractor shall provide support to FSC’s document scanner systems/devices. The Contractor shall:

a.) Analyze VA FSC scanning requirements to also include Debt Management Center (DMC) remote scanning requirements.

b.) Support or perform the process to identify and gather requirements from management officials, customers, and end-users.

c.) Perform or support business analysis to define scanning software system requirements at FSC & DMC.

d.) Perform system and software upgrades.

e.) Perform ongoing maintenance.

f.) Analyze/redesign current implementation to improve efficiency and functionality.

g.) Identify, design, and implement new configurations as new requirements arise.

h.) Design solutions for scanner requirements.

i.) Develop and implement scanner system changes as required by upgrades, component integration or configuration changes.

j.) Implement, maintain, enhance and manage scanner software.

k.) Provide, support and execute detailed Scanning Support test plans for each user level/section of the application.

l.) Test all applications and processes from three perspectives: developer, user and security.

m.) Document and assist with system roll-out to production, and other lower environments as needed, to include all necessary instructions to move the application(s) into production and/or lower environments. Ensure implementation is successful; troubleshoot and resolve any issues with the application.

n.) If there are modifications to the requirements throughout the project, provide an updated user requirements document, security requirements document, and estimated level of effort.

o.) Create and provide Scanning Application User Guides.

p.) Create and provide Scanning Application Administrator Guides – to include a section for Help Desk/Network Administrators, as well as the development team. The information shall be detailed enough that the application could be administered by someone other than the original administrator.

q.) Provide VIP documentation during software development to ensure future developers and administrators can easily understand the software code logic, application usage, and implementation.

r.) Maintain an audit trail of all modifications and updates to scanning applications in the VA-FSC IT Infrastructure.

s.) Maintain product compatibility and compliance with VA security policies, practices and procedures.

t.) Plan, document, test, and execute ISCP procedures.

u.) Provide scanning development and technical support to systems support and development team members.

v.) Troubleshoot and resolve technical problems with the design and delivery of scanner support services.

w.) Provide emergency response services when scanning software systems disruptions occur after normal business hours.

x.) Collect and analyze scanner support services usage and performance statistics.

y.) Perform system data and media conversion.

z.) Keep abreast of current scanning technologies, standards and methodologies.

aa.) Maintain VA-FSC scanning environment, hardware and software, to keep it current with the COTS vendor’s software or version, patches, and security updates.

bb.) Support scanning software projects by developing and implementing the requested functionality and deliver necessary documentation. Those deliverables shall align with VIP.

cc.) Participate in project meetings and activities in support of FSC scanning software projects, software maintenance releases, and emergency software releases.

**Deliverables:**

A. Scanning Application User Guide

B. Scanning Application Administrator Guide

C. Scanning Support Test Plans

### SYSTEM ENGINEERING

The Contractor shall provide system engineering support. The Contractor shall:

a.) Design and manage the complex engineering and integration of the application and/or systems, security, and infrastructure architecture.

b.) Research, evaluate, develop, and implement innovative IT prototypes and solutions to address director and service line stakeholder viewpoints/goals.

c.) Monitor FSC enterprise architecture and computer systems to ensure they are working optimally, and to ensure that the hardware and software used by FSC are compatible with all appropriate VA and Federal policies and procedures.

d.) Manage FSC infrastructure software, system and equipment life cycles, requirements engineering, and capacity planning.

e.) Assist in the development and maintenance of FSC FTS Infrastructure and Application architecture.

f.) Identify departmental needs and make suggestions regarding technical direction.

g.) Design, document, and implement System Security and Data Assurance Processes and Procedures.

h.) Configure and install computer systems as requested by FTS Management.

i.) Test software applications and systems to ensure they meet the necessary engineering requirements to work in an efficient, effective, and secured manner.

j.) Analyze and document FSC current and future users' needs.

k.) Create flowcharts, diagrams, and other documentation on FSC Infrastructure, applications, and systems.

l.) Create manuals and detailed sets of instructions for IT Administrators (Application, System, Data, Network, and Security).

m.) Create and implement a User Experience (UX) metrics and document in the UX Metrics Report.

n.) Develop as-is architecture and to-be capability design and technological roadmaps in conjunction with the enterprise architecture team.

o.) Document and submit weekly accomplishments to be reported under the Weekly Division Status Report under PWS 5.1.3

p.) Update and maintain the System Engineer Project Portal

q) Provide Data Engineering services, to include the following:

1. Use appropriate data sources to address the specific requirements of projects for data modeling.
2. Understand business requirements and translate into technical work.
3. Build ETL jobs and workflows to combine data from disparate sources.
4. Install continuous pipelines of pools of filtered information so that data analyst/scientists can pull relevant data sets for their analyses.
5. Collaborate with business stakeholders, business operations, and product engineering teams in analyzing business problems, building and testing solutions and data models, and in implementing and operating analytic models and services. Perform activities related to Data warehousing, Databricks and big data.
6. Support sandbox/analytics platform and support the file management structure within the environment for modeling and testing.
7. Perform common data wrangling activities, such as parsing, filtering, and transformation. Preprocess data given context of analytic problems.
8. Identify data quality problems with Data Analytic solutions including quality problems with internal and external data sources.

s) Provide support and sustainment for data models and analytic technologies within on prem and cloud environments. Ensure operability and maintenance of all existing developed and development in progress.

t) Provide maintenance and support for Enterprise-wide BI reports with advanced visual analytics, visualizations, multi-level filtering, drill down/drill thru capabilities.

**Deliverables:**

A. System Security and Data Assurance Processes/Procedures upon request

B. Documentation for FSC Infrastructure Application/System upon request

C. Manuals/Sets of Instructions for FSC Infrastructure Application/System upon request

D. UX Metrics Report upon request

### CLOUD SYSTEM ENGINEERING

The Contractor shall provide cloud system engineering by supporting the design, implementation, deployment, operations and maintenance, performance monitoring, and reporting for cloud systems, services, and applications. The Contractor shall also provide support for projects where there is to be a new solution implementation or existing solution/application that is cloud suitable into the VAEC. This task shall be a repeatable process for input of applications and products to be taken into the cloud. The Contractor shall perform the following standard cloud engineering tasks:

a.) Develop business case and requirements for cloud intake solutions.

b.) Analyze alternative approaches and present findings.

c.) Advise VA of cloud suitability.

d.) Complete initial cost estimates.

e.) Assess cloud-readiness.

f.) Assist VA in cloud funding identification.

h.) Support setup, configuration, and provisioning of cloud Environments.

i.) Monitor and track the creation, update, and deletion of user accounts, and ensure cloud capacity requirements are satisfied.

j.) Design VAEC/cloud hosted solutions and address cloud-readiness gaps. The Contractor shall use cloud native approaches as defined in VA’s Use of Cloud-Based Native Technologies and Approaches Policy.

k.) Manage and implement Cloud Provisioning and Management of marketplace applications and services in VAEC.

l.) Manage and control permissions in the cloud service provider for each FSC application, storage, and service being hosted.

m.) Implement, manage, and design monitoring capability of cloud architecture and cloud hosted systems and applications to ensure they are working optimally and that the hardware and software used by FSC are compatible with all appropriate VA and Federal policies and procedures.

n.) Provide a Quarterly Solution Performance Report that summarizes solution availability, usage, events and incidents, improvement opportunities, risks and issues, status, action plans, and planned and actual resolution timelines.

o.) Review all usage of cloud computing services provided by VAEC. The Contractor shall submit and implement Quarterly Resource Utilization Optimization Plans on how to best optimize the environment to reduce the costs associated with resource utilization.

p.) Provide a breakdown of all costs by solution, environment, and utilization. The Contractor shall report on utilization of each class of resource as a percentage of provisioned capacity in a Monthly Utilization Report. The Contractor shall, as part of its Monthly Utilization Report, include the total infrastructure expenditure and total number of request services for Cloud Resource Optimization.

q.) Manage and implement consistent and granular cloud infrastructure security to include system, requirements engineering, and capacity planning.

r.) Assist in the development and maintenance of FSC cloud Infrastructure and Application architecture.

s.) Identify service line and departmental needs and make suggestions regarding technical direction.

t.) Design and implement cloud security and data assurance processes and procedures.

u.) Support setup, configuration, and provisioning of VAEC environments.

v.) Test cloud software applications and systems to ensure they meet the necessary engineering requirements to work in an efficient, effective, and secured manner.

w.) Develop the required A&A documentation for the system and complete VA A&A process. The Contractor shall provide input to update the VAEC ATO, as needed.

x.) Provide information and documentation to support operational and production readiness reviews and go-no-go decisions. The Contractor shall execute corrective actions to address gaps and provide all required data and prepare supporting documents/artifacts for the reviews.

y.) Create data flow diagrams, cloud security diagrams, transition architecture diagrams, and high-level architecture diagrams on Cloud Infrastructure, applications, and systems.

z.) Configure and implement cloud: data backups, DR, load balancers, functions, python, bash, and PowerShell scripting, Cloud Service Provider (CSP) hosted applications and databases services, storage (volume, file, blob, access keys) security permissions, and resource groups.

aa.) Configure and document Cloud Product Operations Manuals (POM) for cloud-based software and systems.

* + 1. Create operations manuals and detailed sets of instructions for IT Cloud Administrators (Application, System, Data, Network, and Security).
    2. For new Cloud implementations/migrations, the Contractor shall also generate an Operations & Maintenance (O&M) Plan to be utilized for continued maintenance of the system/application being transitioned to VAEC.

bb.) Manage cloud system and application implementation, migration, rationalization, transition decommission, and conversion.

cc.) Develop, manage, and maintain an FSC Cloud Migration Plan that addresses architecture, security, data synchronization, and migration of applications, environments, and data. The Migration Plan shall consist of the following:

i. The Contractor’s iterative schedule, sequence of migration tasks, deployment plan, back-out, rollback and recovery plans, and verification and validation activities required to execute the data migration. This will include the Contractor’s implementation approach, processes, and activities (prior to, during, and after), test strategy, setup and configuration procedure, inventory of IT assets, risk assessment, risk log, and key dependencies. The Plan shall include the provisioning and installation procedures for VAEC resources and be compliant with the most current VA Policies and Guidance, which are cited in PWS Section 2.0. If a VAEC CSP has not yet been selected by VA, the Contractor shall recommend a CSP.

ii. For new Cloud implementations/migrations, the Contractor shall also work with VA business owner/stakeholders on elicitation of the testing criteria and use cases to perform UAT. The Contractor shall document this information in the Testing and Validation Plan. Upon approval, the Contractor shall execute.

iii. For New Cloud Implementations, the Contractor shall also develop Transition Checklist that shows access control, security, monitoring, access/permissions are good and turn over POM to the O&M group. Upon completions, the contractor shall transition support to O&M.

iv. Conduct Post-Implementation Review, within 5 days of implementation completion, to review lessons learned and identify improvement opportunities. The Contractor shall provide a Migration Summary Report that describes implementation results, deviations from the Migration Plan, lessons learned, open issues, corrective action, and improvement opportunities.

dd.) Support the execution of the Migration Plan to prepare VA stakeholders to receive and operate the solution. This includes improving stakeholder engagement, outreach, and communications.

ee.) Support setup, configuration, and provisioning of VAEC environments.

ff.) Determine cloud capacity (credits) and workload requirements. VA shall review and approve cloud capacity requirements.

gg.) Create and implement a cloud User Experience (UX) Metrics Report to check and identify metrics and to track and monitor the user experience.

hh.) Provide FSC cloud support services for systems and applications in the VAEC environments (i.e., Microsoft Azure Government (MAG) and Amazon Web Services (GovCloud)), best practices and ensure compliance with VIP development, release, and documentation requirements. This cloud support may be in the form of re-platforming, re-hosting, refactoring, or retiring.

ii.) Use VA Technical Reference Model (TRM) approved tools to build and manage a FSC DevOps pipeline and Infrastructure as Code environment that automates builds, tests, and deployments that meet VA project and VIP requirements. Ensure that all project artifacts are versioned correctly and follow a build release promotion versioning approach which identifies all major, minor, and update changes to the components. Maintain baselines of software, software builds, and electronic artifacts and ensure all code is checked in compliance with VA requirements: One-VA TRM, VA 6500, VA Enterprise Design Patterns Cloud Computing and Cloud Computing Architecture, and the VIP.

jj.) Support development and documentation of capability and technology roadmaps, application and system rationalization, and cloud and capability migration mapping.

kk.) Coordinate and support updates for the FSC service catalog including documentation of the data tags used for applications hosted in the VAEC.

ll.) For new Cloud implementations/migrations, the Contractor shall develop and maintain the solution architecture and ensure alignment with the One-VA Enterprise Architecture and VAEC Technical Reference Architecture, and document in the Design and Architecture Plan.

**Deliverables:**

A. Quarterly Solution Performance Report

B. Quarterly Resource Utilization Optimization Plans

C. Monthly Utilization Report

D. Cloud POMs

E. Operations & Maintenance (O&M) Plan

F. FSC Cloud Migration Plan

G. Testing and Validation Plan

H. Transition Checklist

I . Migration Summary Report

J. User Experience (UX) Metrics Report

### ENTERPRISE ARCHITECTURE STRATEGY SUPPORT

The Contractor shall support the development of the Financial and Acquisition Segment Architecture that follows the Federal Enterprise Architecture Framework (FEAF) and VA Architecture Framework (VAAF). Architecture support shall leverage a series of standards and reference models in compliance with FEAF and VAAF. The architecture shall be developed using FEAF (v2.0+), the Department of Defense Architecture Framework (DoDAF) (v2.02) and other Fit-For-Purpose (FFP) formats.

The Contractor shall review existing Architecture methodology that enables a repeatable agile process that supports the development of integrated architecture domains and linkages with core financial management and acquisition support systems. The Contractor shall review existing current, interim, and target state architecture information for analysis to ensure traceability across business, data, organizational, security and system/interfaces domains. The Contractor shall also update existing Architecture information as needed to ensure accuracy and completeness.

The Contractor shall provide recommendations on the interim and target state implementation plans that are aligned and synergistic to other Architecture Segments (i.e., Health) and the Enterprise Architecture.

The Contractor shall support the execution of the Architecture Strategy and shall review established Architecture Governance to provide technical feedback on the design, development, and deployment of the Architecture/Segment Architecture including over each lifecycle. The Contractor shall make recommendations to Architecture Governance structure within the Segment if improvements are necessary. The Contractor shall provide a Segment Architecture Recommendations Report which will review established Segment Architecture Governance, Methodology and Strategy against existing segment architecture and make recommendations for improvements to enable accurate, complete Financial and Acquisition Segment development that is aligned with Enterprise and Cross Segment Architecture. The Contractor shall perform Architecture Interrogative to facilitate collection and usage of architecture-related data. The Contractor shall provide communication on Architecture/Segment Architecture governance, methodology and strategy as needed to solution architects of the various architecture domains (i.e., business, data, systems) within the Financial and Acquisitions segment. The Contractor shall provide training as needed to ensure that architects are adhering to Architecture/Segment Architecture governance, methodology and strategy to enable the Contractor can successfully build the Architecture/Segment Architecture. Through monthly communications, the Contractor shall provide visibility into the progress of the development and uses of the Segment Architecture in layman terms. Further, the Contractor shall provide Segment Architecture Training Materials that will enable use of architecture-related data by various levels of users (i.e., planners, owners, designers, builders)

The Contractor shall develop and provide Segment Architecture Blueprints and Architecture Models necessary to establish and execute the Segment Architecture for current, interim and target states. The Contractor will utilize the captured architecture to provide the following models:

* + Performance Reference Model (PRM) Architecture
  + Business Reference Model (BRM) Architecture
  + Data Reference Model (DRM) Architecture
  + Application Reference Model (ARM) Architecture
  + Infrastructure Reference Model (IRM) Architecture
  + Security Reference Model (SRM) Architecture
  + Architecture Blueprints
  + Architecture Viewpoints and Models
  + Architecture Interrogatives

**Deliverables:**

A. Segment Architecture Recommendations Report

B. Segment Architecture Training Material

C. Segment Architecture Blueprints and Architecture Models

### SOLUTION ARCHITECTURE IMPACT ASSESSMENT SUPPORT

The Contractor shall support impact assessment by conducting architecture analytics on the integrated Financial and Acquisition Segment Architecture information gathered, standardized, integrated, and developed by the Segment Architecture Team. The Contractor shall conduct analysis of segment architecture across the various solution level domains (i.e., business, data, systems, etc.) and additional data points (i.e. system cost analysis). Areas of analysis include reviewing the Interface Strategy Executive Overview to validate the Business Process Reengineering (BPR) legacy system disposition recommendations and validate that the interface disposition recommendations are the best recommendation within the understanding of the Segment and Enterprise Architecture context. Further, in support of reviewing the current state systems, the Contractor shall review interfaces architecture and recommend interim and target state systems and interfaces architecture that are more streamlined and will improve overall system performance (i.e., reducing data exchange traffic and time).

The Contractor shall conduct descriptive and predictive analytic routines to determine the impact of modernizing and transforming business, system, security, data, infrastructure, and organization components that enable financial and acquisition activities to occur. These analytics will inform leadership on the most efficient and effective decisions to make based on the architecture information gathered. The analytics will also help designers and developers inform and check their work. The Contractor shall conduct requirements elaboration and validation for each architecture domain to determine the analytics reports are useful for the business domain and different level of users. The Contractor shall also support education and training to the program on the rationale and objectives of the analytics efforts. The Contractor shall communicate to stakeholders on the results of the analytics by providing a Segment Architecture Analytics Reports and the Segment Architecture Analytics Training Material.

The Contractor shall support information gathering sessions in collaboration with the solution architecture team. Support shall include working with stakeholders to complete necessary as-is, interim and target state documentation and templates, coordinate and facilitate analysis sessions, review relevant administration or staff office enterprise and system architecture, and analyze collected data to recommend interface disposition recommendation, integration, and implementation approach. The Contractor shall also interface with other sources of information such as the VA Enterprise Repositories, cost analysis data spreadsheets.

**Deliverables:**

A. Segment Architecture Analytics Reports

B. Segment Architecture Analytics Training Material

### ORGANIZATIONAL ARCHITECTURE SUPPORT

The Contractor shall provide the following Organizational Architecture Support services for FSC, and its customers as required. These services shall include but shall not be limited to:

a.) Select reference models, viewpoints, and tools.

b.) Develop and document the Baseline Business, Application, Data and Technology Architecture Descriptions.

c.) Develop and document Target Business, Application, Data and Technology Architecture Descriptions.

d.) Perform gap analysis between items b.) and c.)

e.) Define Candidate roadmap components and create transition architectures.

f.) Resolve impacts across the architecture landscape.

g.) Conduct formal stakeholder reviews.

h.) Finalize Business Architectures.

i.) Create Architecture Definition Documents.

j.) Perform EA Governance.

k.) Develop and implement architecture vision.

l.) Develop and implement business architecture.

m.) Develop and implement information system architecture.

n.) Develop and implement technology architecture.

o.) Develop and implement opportunities and solutions.

p.) Develop and implement migration planning.

q.) Develop and implement architecture change management.

r.) Develop and implement architecture requirements management.

s.) Perform the analysis of business structure and processes.

t.) Design, develop, implement, and sustain data, application, business, and technology architecture models. These models shall be architected at the following layers: conceptual, logical, business area, and application.

u.) Develop and deliver long-term strategic goals, product and service road maps, service catalogs, and standards.

v.) Create short-term tactical solutions to achieve long-term objectives and an overall management and transition roadmap.

w.) Establish processes for governing the identification, collection, and use of corporate metadata; take steps to assure metadata accuracy and validity.

x.) Establish methods and procedures for tracking quality, completeness, redundancy, and improvement.

y.) Create strategies and plans for data, application, business, technology security.

z.) Ensure that strategies and architectures are in regulatory compliance.

aa.) Assess and identify applicable governance, stewardship, and frameworks for managing data, application, business, and technology architecture across the organization with a focus on identifying and developing opportunities for reuse, migration, or retirement.

bb.) Prepare EA business case, exposes benefits and drivers, financial merits.

cc.) Present, justify, and communicate to all stakeholders in business and IT.

dd.) Specify EA framework, best practices, and tools.

ee.) Establish architecture, design and technology principles and guidelines.

ff.) Participate in EA design and development.

gg.) Control the consistency and compliancy of artifacts.

hh.) Perform the FSC EA repository management. and management of access rights.

ii.) Recommend transformation roadmap and work with VA FSC Program Management Office

jj.) Control EA iterations deliveries

kk.) Establish compliance checkpoints in major capability development processes.

ll.) Assess EA maturity.

mm.) Measure returned value at each iteration or transition.

nn.) Perform the mapping of data sources, data movement, interfaces, and analytics, with the goal of ensuring data quality.

oo.) Document the data, application, business and technology architecture and environment.

pp.) Develop and maintain the FSC Service Catalog, documenting business line service definitions, applications, services, associated service level agreements (SLA)s, and service level metrics.

**Deliverables:**

A. Baseline Business, Application, Data and Technology Architectures

B. Target Business, Application, Data and Technology Architectures

C. Technology Roadmaps

D. FSC Service Catalog

### SYSTEMS ANALYSIS SUPPORT

The Contractor shall:

a.) Interview and conduct meetings with management officials, customers, and end- users to define and document requirements.

b.) Perform business analysis to define business, functional and software system requirements.

c.) Obtain customer and Project Manager approval for requirements and project planning documentation before forwarding documents to the development team.

d.) Communicate business and functional requirements to technical staff.

e.) Review requirements to identify specific system and software upgrades required.

f.) Perform systems analysis activities in support of ongoing systems and application maintenance and sustainment; produce Systems Analysis Reports

g.) Provide analysis and redesign input on current implementations to improve efficiency/functionality.

h.) Provide analysis support on implementation of new systems configurations as new requirements arise.

i.) Analyze, assess and document FSC business processes and advise FSC management on areas of improvement in an FSC Business Processes Review and Recommendations Report.

**Deliverables:**

A. Systems Analysis Reports

B. FSC Business Processes Review and Recommendations Report

### EDI HELP DESK/OPERATIONS SUPPORT SERVICES

The Contractor shall provide tier 1 and tier 2 level support for production jobs and applications including identifying issues (incidents), addressing issues based on roles and responsibilities, documenting impacted applications and customers, and communicating issues and impact to FTS management, co-workers, and customers. The Contractor shall ensure issues are addressed and resolved, creating, updating, and closing necessary trouble tickets, incidents, or change requests to track incidents, and providing final resolution communication to FTS Management, co-workers, and customers. The Contractor shall:

a.) Support processing of EDI transactions using the Accredited Standards Committee (ASC) X12 Healthcare and Supply Chain standards, Fast Healthcare Interoperability Resources (FHIR), the National Council for Prescription Drug Programs (NCPDP) standards, JavaScript Object Notation (JSON), and the Health Level 7 (HL7) protocol.

b.) Communicate with trading partners (e.g. commercial vendors, healthcare payers and providers, utility providers), customers and change requestors and log all Requests for Change (RFC), inquiries, and customers’ requests in ServiceNow or any other tool specified by FTS management. Provide ticket status to customers or requestors on a regular interval as specified by FTS management until ticket is resolved.

c.) Perform initial triage for production issues, document results of triage on trouble ticket, and escalate issues to tier two when unable to resolve issue.

d.) Maintain VA-FSC EDI Team group mailboxes and/or telephone line.

e.) Update the Weekly ServiceNow Ticket Report in PWS 5.2.5.6, and produce the Monthly EDI Transaction Volumes Report and other reports as requested using templates provided by FSC.

f.) Perform application monitoring across various platforms such as Mainframe, Windows/Linux Servers and Cloud to ensure they are running as scheduled. Respond to issues or problems preventing jobs and applications from running as expected.

g.) Notify VA FTS management of critical incidents and system outages at time of incident, manage recovery/resolution activities related to the incident and provide status updates until incident is resolved.

h.) Provide Root Cause Analysis (RCA) documentation following system outages and critical incidents.

i.) Follow established FTS procedures, update and create procedures to keep documentation current.

**Deliverables:**

A. Monthly EDI Transaction Volumes Report

### EDI APPLICATION SUPPORT

The Contractor shall implement, configure, administer, and support designated VA-FSC EDI applications, systems, COTS software and tools, which currently include:

a.) COBOL, DYL260, DYL280 and SyncSort.

b.) Foresight EDISIM and Foresight Instream.

c.) Compuware products - including FileAid and AbendAid IBM CICS.

d.) Roger Software Development Enterprise Output Solution.

e.) IBM z/OS version 2.1.6, including PKZIP, Librarian, JES3, JCL.

f.) Mainframe File structures - including Generation Data Group (GDG), Partition Data Set (PDS), Virtual Storage Access Method (VSAM), and Statistical Analysis System (SAS).

g.) Translators - MuleSoft, Gentran Translator, Vitria BusinessWare, Trusted Link Enterprise (TLE), or other data translator.

h.) Communication packages - DMI, Mailman, Cleo’s VL Trader, IBM Sterling Connect: Direct.

i.) Transmission protocols - AS2, SFTP, HTTPS, SSH, SOAP, TCP/IP, Connect: Direct, etc.

j.) Software - Oracle TOAD, Microsoft SQL Server Management Studio, Text Pad, UltraEdit, SOAPUI, SharePoint, Rally, Rational, Tibco Instream Validator.

k.) Languages - J2EE, Java and Oracle Script.

The Contractor shall support tier one and tier two production support activities including:

a.) Incorporating into existing solutions production control processes that identify problems and provide prompt resolution, using six-sigma processes improvement techniques as necessary. Creates user stories and/or documents defects in Rally/Rational, or any other tool required by the COR, to support production support efforts.

b.) Maintaining and creating EDI Application Documentation and ensuring that documentation is easily accessible and current;

c.) Differentiating between issues with system performance and changes to existing functionality to properly prioritize and triage the issues.

d.) Conduct testing to add new trading partners to existing EDI solutions including but not limited to the following documents types: invoices, payments, purchase orders, healthcare claims, healthcare eligibility, healthcare payments, pharmacy claims, and prior authorizations.

e.) Support the completion of MOU/ISA, BAA or any other documentation to support implementation of processes to exchange electronic transactions with trading partners.

The Contractor shall assist in EDI Systems, Lifecycle Management for all processes, practices, and methods under which the VA-FSC EDI services are designed, developed, tested, integrated, operated, documented, and maintained. This includes completing and/or conducting peer reviews of systems and application documentation including Concept of Operations, Production Operation Manuals, Security Reviews, 508 Compliance Reviews, Software Design Document, and Deployment plans.

**Deliverable:**

A. EDI Application Documentation

## DATA ANALYTICS SUPPORT

The Contractor shall use data management, data mining, statistical analysis, and visual analytics software currently in use at FSC or available to FSC like Structured Query Language (SQL), Audit Control Language (ACL) data analysis software, Databricks, R, Statistical Analysis System (SAS), Python, Tableau, and a myriad of related analytical technology/methods. The Contractor shall provide DAS support services to perform timely data analysis, analytics, forecasting, and support of tools to achieve continually evolving analytics that support program planning, evaluation, and analyses of various programs, projects, budgets, performance, project execution, transition, reports, visualization, and risk mediation workflows.

### DATA ANALYSIS AND BUSINESS INTELLIGENCE

The Contractor shall provide technical expertise in the data development of a wide range of analytic solutions and products, which shall include expertise in and provision of visual solutions, such as Microsoft Power BI, as well data development of analytic products using the full spectrum of descriptive, diagnostic, predictive, and prescriptive analytic methods. The Contractor shall use contemporary methods of data profiling, exploratory data analysis (EDA) and quality assessments to enable the VA-FSC to effectively meet DAS program goals. Contractor shall use machine learning and artificial intelligence enabled capabilities to proactively detect data anomalies and trigger a system response to prevent data corruption. The Contractor shall use an iterative approach in refining the analytic solution to meet customer needs. The Contractor shall provide data science, data engineering, project management, business intelligence and analytic services support. Specific analytic solutions include dashboards, application, and automation services, as well as the full spectrum of analytic methods required for VA-FSC customers, including descriptive, diagnostics, predictive and prescriptive approaches.

The Contractor shall use industry standards in data analytics and business intelligence to meet VA-FSC business requirements. The Contractor shall serve as facilitator in resolving discrepancies and data quality issues with subject matter experts (SMEs), customers, and program owners. The Contractor shall support the rollout of enterprise level data analytics and business intelligence services in accordance with DAS’ analytic needs.

1. Solution data development methods: The Contractor shall use a team-based, Agile analytics framework in the data development of all work products. The Contractor shall utilize best practices in solution data development, which may include concepts such as scrum, XP, Kanban, and related approaches and shall optimize delivery of products through use and evaluation of the methods. The Contractor shall utilize management tools selected by the Government such as JIRA or Agility for the development of analytic products. The Contractor shall use management tools and align utilization with analytic solution data development as framed by analytic data development process model. The Contractor shall employ data analytics, data management, and Master Data Management (MDM) solutions to consolidate, master, and synchronize core customer data across multiple disparate data sources using a variety of technologies.
2. Application domain understanding: The Contractor shall facilitate the development of business requirements into analytic goals through a thorough assessment of business problems; through defining business objectives and translating into analytic goals; and, through identification of key stakeholders, current solutions, and domain technology. The Contractor shall document the business requirements in the Project Plan and shall refine them throughout the planning, modeling, and analysis process. The Contractor shall guide the partitioning of the analytic solution into smaller tasks that can be solved using an agile approach to solution delivery.
3. Data understanding: The Contractor shall identify data quality problems; identify internal and external data sources; and select subsets of data relevant for meeting business requirements through data development of an analytic solution. The Contractor shall collect data, verify data completeness, identify redundancies, statistically adjust for missing values, and assess utility of the data with respect to analytic goals. The Contractor shall provide an analysis of accessibility and availability of data, selection of relevant data attributes, and processes for storing and managing data. The Contractor shall conduct data profiling and EDA in support of data development of the analytic solution. The Contractor shall identify and report implementation constraints, such as computational frequency, solution timeliness, data storage limitations, and computational resource limitations.
4. Data preparation and identification of analytic technologies: With Government approval before enacting, the Contractor shall select the most appropriate analytic method(s) solution given business requirements, organizational context, operational barriers, and other relevant considerations. The Contractor shall identify execution models based upon refresh cycles (e.g., batch vs. streaming). The Contractor shall utilize the VA On-Premise environment and Cloud environment and shall support and sustain the models and analytic technologies within those environments. The Contractor shall support the sandbox/analytics platform and shall also support the file management structure within the environment for modeling and testing. The Contractor is responsible for developing synthetic test data to mock partner systems and support performance testing. The Contractor shall perform Extract, Transform, and Load (ETL) and Extract, Load, and Transform (ELT) processes. The Contractor shall perform common data wrangling activities, such as parsing, filtering, and transformation. The Contractor shall preprocess data given context of analytic problem, which may include the following activities:

* Outlier adjustment
* Adjust for missing values through imputation or other means
* Address noisy data
* Conduct data processing (e.g., transformation)
* Dimensionality reduction
* Data aggregation
* Data enrichment

1. Data modeling: The Contractor shall apply the selected analytic method(s) to the prepared data and calibrate and test as appropriate to evaluate goodness of fit, multicollinearity, normality, heteroscedasticity, and related statistical features. The Contractor shall use data mining and learning analytic methods, such as regression, clustering, and classification. The Contractor shall use contemporary and traditional methods in linear modeling (e.g., GLM), forecasting, econometrics, survival analytics, discrete choice modeling, categorical data analysis, and nonparametric analysis. The Contractor shall use appropriate simulation and optimization modeling techniques, to include geospatial simulation. The Contractor shall use SQL, Microsoft Power BI, R, Python, SPSS, SAS, and related applications to develop the product, analyze and visualize data. The Contractor shall integrate statistical and quantitative models into the Business Intelligence platform in business-friendly and accessible ways. The Contractor shall test products using a Government witness of the testing and testing shall be deemed completed when testing demonstrates the product operates in agreement with a test plan and upon government approval of the test results.
2. Evaluation: The Contractor shall interpret results of the analysis based on visualization of results, examination of goodness of fit measures, examination of variation reduction, and other means. The Contractor shall review, and revise data models and structures as required to ensure model integrity.
3. Knowledge consolidation and deployment: The Contractor shall support the deployment of the analytic product and present the generated knowledge in a business-oriented way. Delivery of the final product may include a visualization (dashboard) or statistical summary, but in either case shall be attainable for the lay business reader. The Contractor shall leverage knowledge acquisition and facilitate the incorporation of knowledge and methods into the VA system. The Contractor shall support monitoring and maintenance of the product and identify means to extend the results from the current to other possible domains. Contractor will provide step-by-step Pre-Deployment Checklist prior to deployment of data sets and reporting.

The Contractor shall:

* Document all Technical Specifications of all scripts, codes used in ETL, ELT processes.
* Deliver all Final Models used for each analytic product in the language used for the product (i.e., provide R, Python documentation).
* Generate and support the data development of recurring and ad hoc reports as requested. (EX: Data Reconciliation Reports, Data Matching Reports, Financial Accounting Reports).
* Thoroughly document and train Federal Staff on the backend data operations/functionality, BI solutions data development, and maintenance activities to ensure consistency in designing, developing, delivering, and deploying customer and enterprise BI solutions.

Deliverables:

A. Pre-Deployment Checklist

B. Technical Specifications

C. Final Models

### DATA ANALYTICS CUSTOMER SUPPORT

The Contractor shall provide customer support to sustain and maintain the functionality of deployed or existing data analytics and business intelligence products. The Contractor shall document, track, and resolve customer issues and provide monthly updates to the Issue Tracking Log. In addition, the Contractor shall establish a Customer Support Log that documents who is being helped, what work is required, when started and completed, and how many hours spent assisting the customer. The Contractor shall support efforts to provide updates to the customer base via an interactive communication portal on issues that affect a product/product line.

The Contractor shall ensure that all sustained products be continuously considered for optimization. If the products fall below best practice, the Contractor shall provide proposed optimizations that will be submitted within 30 days of identification of the optimization. Data Analytics Service has products active in 4 main areas. The existing products are in Power BI and have varying levels of data and complexity.

Sustainment products include: multiple Enterprise-wide BI reports with advanced visual analytics, multi-level filtering, drill down/drill thru capabilities. Enterprise reports are designed and developed to be used universally across VA. Current products include the restricted/non-restricted reporting suite that provides KPI’s, metrics, and operational analytics for financial transactions. There are 100+ visualizations within the current BI solutions in production. Products are operational and currently in use by financial operators.

Business Intelligence (BI) work in data development is as follows: Administrative Specific BI solutions which are designed and customized to be used by a sole administration to address its individual reporting requirements. Work in data development includes 47+ visualizations, connecting three VA systems of records, to build BI solutions to help modernize invoice payment reports, resourcing forecasting, and end-state projections to start. The BI products/project data development work is prioritized in real time to meet future customer needs.

**Deliverables:**

A. Issue Tracking Log Update

B. Customer Support Log

### DATA MANAGEMENT AND GOVERNANCE

The Contractor shall provide support in planning and developing a data management and governance capability for the FSC’s DAS independent of project assignments. The Contractor shall support existing and emerging data governance structures while serving a critical role of facilitation of data stewardship. The Contractor shall collaboratively work with key stakeholders from appropriate levels, determined by FSC DAS Leadership, across the VA organization to enable the development of an effective enterprise data governance program. The Contractor shall support business management administration and executive leadership by supporting strategic planning, integration management, data development activities and implementation in the field of data management and governance. In the coordination of data management activities, the Contractor shall schedule meetings, plan, and publish agendas, develop, and provide documents for review, facilitate meetings, track issues, follow up on decisions, and publish meeting minutes. The Contractor shall support recurring meetings with stakeholders and leadership at local and senior levels of VA, with an expected meeting load of 2–4 meetings/month. The Contractor shall support development of a data strategy, data policies, data architecture, and data standards and procedures and document these results in the Data Governance and Management Documents. Policies will cover areas such as data sharing; data quality standards, roles and responsibilities; data modelling; general data access and usage; data access by external parties, and related topics. The Contractor shall support and develop control mechanisms that span a tiered approach to data governance, which include but are not limited to the identification, capture, logging and updating of requirements and issues; tracking the status of issues; documenting stakeholder views; escalating issues with recommendations to higher levels of authority; and documenting issue resolutions. The Contractor shall serve as a member of, or provide Subject Matter Expertise to, Integrated Product Teams (IPTs) or other organizational structures for the purpose of providing insight to data analysis process. These structures are cross-functional teams that work collaboratively to develop strategies and approaches to meet objectives. The Contractor shall provide expert guidance across a range of domains included in the data management (DM) field, to include data quality, data governance, data stewardship, master data management, business intelligence and analytics, and related DM focus areas.

In addition, the Contractor shall:

1. Update and maintain the Data Management Roadmap. This will identify specific programs, tasks assignments, stakeholders, and communications for various data sets.
2. Contractor shall be responsible for maintaining DAS communication content such as current data governance, knowledge management, and other DAS initiatives and information utilizing existing internal and external communication tools.
3. Log and track data management issues including issues related to: data quality, business rule conflicts, decision rights and other potential data issues. This information shall be captured, tracked, and reported monthly in the Issue Management Log which will be updated in the Interactive Communications Portal.
4. Utilize a standardized framework to identify current and future gaps in FSC’s data governance and management and provide reports and recommendations. Reports shall include status on current efforts, plans, stakeholders, task assignments, issues, and mitigation strategies.
5. Work to the adoption of an Open Data Framework to enable a modern and scalable data architecture. The framework should support business intelligence and analytics; data profiling and meta data practices; data ingest pipelines; data lake; data abstraction and sharing; data security; and data quality improvements.
6. Work to codify and document meta-data.

**Deliverables:**

1. Issue Management Log

## PRIVACY SERVICE

FSC FTS supports numerous systems, applications, and data that must be properly managed and secure to ensure privacy regulations are met. FSC requires technical support on issues related to privacy as they arise. The Contractor shall provide subject matter expertise on privacy topics as required. The Contractor shall:

a.) Maintain and support Privacy Management Program and privacy focused operations.

b.) Identify and recommend improvements to the Privacy Management Program and implement any changes approved by FSC management.

c.) Support implementation of Privacy policies and procedures mandated by VA or federal regulation.

d.) Maintain and support established FSC Privacy policies and procedures as requested by FSC management that comply with VA and federal regulations.

e.) Design Privacy Risk Management into the privacy capabilities of all information systems throughout the system development life cycle used at the FSC.

f.) Monitor compliance with all Privacy policies and procedures.

g.) Identify, document, and address Privacy issues or violations in the Privacy Issues and Violation Report

h.) Identify and recommend privacy controls and tools with the goal of strengthening the FSC posture in this area to protect data.

The Contractor shall lead and/or support multidisciplinary team(s), which collaborate closely with all internal and external stakeholders, and understand the potential values and privacy risks of the emerging digital business. In support of this task, the Contractor shall:

1. Document, support and provide input to the development, implementation, maintenance, and adherence to the organization’s policies and procedures covering the privacy, access, and authorization to data in compliance with federal and state laws and the organization’s information privacy practices. This shall be documented in the Privacy Management Plan.

2. Perform initial and annual information privacy risk/impact assessments and conduct related ongoing compliance monitoring activities in coordination with VA FSC’s other compliance and operational assessment functions, and document findings in the Privacy Risk Impact Assessment Report.

3. Work with the privacy office, FTS management, service lines, and committees to ensure that the organization has and maintains appropriate privacy and confidentiality consent, authorization forms, and information notices and materials reflecting current organization and legal practices and requirements.

4. Document privacy data compliance process and data flow authentication for systems and data.

5. Participate in the development, implementation, and ongoing compliance monitoring of all data trading partner and business partner agreements to ensure all privacy concerns, requirements, and responsibilities are addressed.

6. Review system-related information documents such as system security plans and POMs throughout the organization to ensure alignment between security and privacy practices

7. Act as a liaison to the Engineering and Infrastructure departments.

8. Work with organization personnel involved with any aspect of release of PHI, PII, and all other sensitive data to ensure full coordination, cooperation, and compliance with the organization’s policies and procedures and legal requirements.

9. Maintain current knowledge of applicable Federal and state privacy laws, accreditation standards, and monitors advancements in information privacy technologies to ensure organizational adaptation and compliance.

The Contractor shall perform these tasks in accordance and compliance with all Federal and VA privacy regulations policies which include but are not limited the below:

• National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2 as a guideline for establishing the Security and Privacy Management program

• Health Insurance Portability and Accountability Act (HIPAA)

• Health Information Technology for Economics and Clinical Health Act (HITECH)

• Electronic Communications Privacy Act

• NIST 800-53 Privacy Section

• Electronic Communications Privacy Act of 1986

• Non-disclosure federal statutes

• OMB Circular A-130

• Government Paperwork Elimination Act

• VA and Federal user authentication, insider threat, and identity theft, and

• Any new or updated Privacy related federal laws, regulations, and publications that may be implemented during performance of this Task Order.

**Deliverables**

A. Privacy Issues and Violation Report

B. Privacy Management Plan

## TRANSITION-OUT SUPPORT (OPTIONAL TASK)

It is anticipated that some work requirements will be in progress at the end of the performance period of this task order. Interruptions or delays to the work will adversely impact the mission. It is essential that attention be given to minimizing the interruption. Therefore, the Contractor shall provide for maximum cooperation between itself and any Government or Contractor staff that may take over performance of this work at the completion of the performance period to ensure that no work receives inadequate attention. The Contractor shall plan for the transition of work to ensure continuity of services at the completion of this TO.

Specifically, the Contractor shall provide 45 days of transition support to ensure a smooth transition to either the Government or a third-party Contractor. The Contractor shall assist with the development of plans, procedures, and methods for assumption of all on-going work. The Contractor shall provide an orderly transition of work acceptance and accomplishment so that full control by the successor is achieved within 45 days of this option being exercised.

Upon execution of this optional task, the Contractor shall conduct analysis, create the strategy, and develop the plans and products needed to successfully transition the provision of services. The Contractor shall:

1. Minimize transition impact to the user community.

3. Maintain existing service quality and performance levels.

4. Ensure a transparent and seamless transition.

5. Maintain support and meet delivery milestones of ongoing projects.

6. Minimize operations and maintenance (O&M) cost overlaps.

7. Ensure that the IT security posture during transition is maintained at current levels without creating gaps and/or vulnerabilities.

8. Ensure no service disruption or degradation during transition.

The Contractor shall develop and provide a Transition Plan covering transition out activities to include strategies and processes needed to maintain continuity of operations and quality of service during the transition in period. The Contractor shall then implement the detailed transition strategies and processes needed to enable at transfer of services from the incumbent service provider to the service platform without disruption to ongoing support levels.

The Contractor shall develop and implement detailed transition. For planning purposes, the overall transition period shall not exceed forty-five (45) days, and transition of operational capabilities shall be completed within that time.

At the request of the COR, the Contractor shall conduct an inventory of GFE and IT assets; establish management processes and controls; and other tasks the Contractor and/or the COR deem necessary to support the transition process.

**Deliverable:**

A. Transition Plan

# GENERAL REQUIREMENTS

## ENTERPRISE AND IT FRAMEWORK

### VA TECHNICAL REFERENCE MODEL

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

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), [https://www.ea.oit.va.gov/EAOIT/VA\_EA/Enterprise\_Technical\_Architecture.asp](https://www.ea.oit.va.gov/EAOIT/VA_EA/Enterprise_Technical_Architecture.asp" \o "Link to One-VA Enterprise Technical Architecture), and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, <https://www.oit.va.gov/library/recurring/edp/index.cfm>. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in VA Handbook 6510 VA Identity and Access Management, VA Handbook 0735 Homeland Security Presidential Directive 12 (HSPD-12) Program, and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

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

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-05-24, M-19-17, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-05-24 and M-19-17 can be found at: <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf>, and <https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf> respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

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

1. Automated provisioning and are able to use enterprise provisioning service.
2. Interfacing with VA’s Master Person Index (MPI) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion-based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VIEWS 00155984, PIV Logical Access Policy Clarification <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>.

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

### INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support Internet Protocol Version 6 (IPv6) based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (<https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf>). IPv6 technology, in accordance with the USGv6 Program [(https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1](file://R04.med.va.gov/V03/EAS/Users/vhaeasWymbsk/TEMPLATES--NEW%20TAC%20PROCESS/PWS%20TEMPLATE%20(DO%20NOT%20TOUCH)%20-%20In%20Process%20Revisions/DO%20NOT%20TOUCH%20(next%20version/IPv6/(https:/www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1)), NIST Special Publication (SP) 500-267B Revision 1 “USGv6 Profile” (<https://doi.org/10.6028/NIST.SP.500-267Br1>), and NIST SP 800-119 “Guidelines for the Secure Deployment of IPv6” (<https://doi.org/10.6028/NIST.SP.800-119>), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices shall support native IPv6 and dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and dual stack (IPv6 / IPv4) operations.

### TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative“ (<https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf>), VA Directive 6513 “Secure External Connections”, and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (<https://www.cisa.gov/publication/tic-30-core-guidance-documents>). Any deviations must be approved by the VA TIC 3.0 Working Group at [vaoisesatic30team@va.gov](mailto:vaoisesatic30team@va.gov).

### STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 10 (64bit), Edge (Chromium based), and 365 Apps for enterprise.  Applications delivered to VA and intended to be deployed to Windows 10 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using Microsoft Endpoint Configuration Manager (CM) VA’s current desktop application deployment tool.  Signing of the software code shall be through a vendor provided certificate that is trusted by VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign.  The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

### VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM)

The Contractor shall support VA efforts IAW the updated Veteran Focused Integration Process (VIP) and Product Line Management (PLM). The major focus of the new VIP is on Governance and Reporting and is less prescriptive, with a focus on outcomes and continuous delivery of value. Product Line Management (PLM) is a framework that focuses on delivering functional products that provide the highest priority work to customers while delivering simplified, reliable, and practical solutions to the business, medical staff, and our Veterans. The VIP Guide is a companion guide to the PLM Playbook and can be found at: <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371> and the PLM Playbook can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>. The PLM Playbook pivots from project-centric to product-centric delivery and contains descriptive practices that focuses on outcomes. The PLM Playbook contains a set of “plays” that implement Development, Security, and Operations (DevSecOps) principles and processes such as automated development, continuous integration/continuous delivery, and release on demand. The PLM Playbook details how product lines implement Lean-Agile principles, methods, practices, and techniques through levels of maturity. VIP and PLM are the authoritative processes that IT projects must follow to ensure development and delivery of IT products.

### PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the FSC Process Repository. The Process Repository serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the FSC workforce, Government and Contractor personnel. The Contractor shall follow the PAL processes to ensure compliance with policies and regulations and to meet VA quality standards. The FSC Process Inventory can be found at [Financial Technology Service - FTS Process Repository - FTS User (sharepoint.com).](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdvagov.sharepoint.com%2Fsites%2FOITFSC%2FOIT%2FFTS%2520Process%2520Repository%2FForms%2FFTS%2520User.aspx%3Fviewid%3Da7456edf-541a-4370-a6af-fd2850bf249e&data=05%7C01%7C%7Cad6b0744609649c99a8808dbcf57e419%7Ce95f1b23abaf45ee821db7ab251ab3bf%7C0%7C0%7C638331748613919157%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=KVOHSweIbee9tyQk6C4azRwrkllt1dIXASDfBAK6qp8%3D&reserved=0)

### SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the ICN in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

## SECURITY AND PRIVACY REQUIREMENTS

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

### 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 |  |  |  |

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

### CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
2. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
3. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
4. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
5. Optional Form 306
6. Self-Certification of Continuous Service
7. VA Form 0710
8. Completed SIC Fingerprint Request Form
9. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
10. The Contractor employee shall certify and release the e-QIP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
11. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. If damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
12. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed “Contractor Rules of Behavior”, and with a valid, operational PIV credential for PIV-only logical access to VA’s network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.
13. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
14. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
15. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

**Deliverable:**

1. Contractor Staff Roster

## METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: Microsoft 365, MS Word 2000/2003/2007/2010/2019, MS Excel 2000/2003/2007/2010/2019, MS PowerPoint 2000/2003/2007/2010/2019, MS Project 2000/2003/2007/2010/2019, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010/2019, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

## 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** |
| --- | --- | --- |
| 1. Technical / Quality of Product or Service | 1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products 5. Incorporates “ease of use” Human Centered Design principles in any software developed. | Satisfactory or higher |
| 1. Project Milestones and Schedule | 1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems | Satisfactory or higher |
| 1. Cost & Staffing | 1. Currency of expertise and staffing levels appropriate to perform tasks required 2. Personnel possess necessary knowledge, skills, and abilities to perform tasks | Satisfactory or higher |
| 1. Management | 1. Integration and coordination of all activities to execute effort | Satisfactory or higher |

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

## FACILITY/RESOURCE PROVISIONS

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

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

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

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

## 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 effort, the Government estimates that the following GFE will be required by this effort:

1. 200 laptops
2. 40 Mobile Phones

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

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

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

# ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

1. Cyber and Information Security Requirements for VA IT Services

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

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

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS) 2.0, and will be tracked therein. The TMS 2.0 may be accessed at [h](https://www.tms.va.gov/SecureAuth35/" \o "Link to TMS 2.0 Homepage)[ttps://www.tms.va.gov/SecureAuth35/](https://www.tms.va.gov/SecureAuth35/" \o "Link to TMS 2.0 Homepage)

. If you do not have a TMS 2.0 profile, go to

<https://www.tms.va.gov/SecureAuth35/>

and click on the “Create New User” link on the TMS 2.0 to gain access.

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

1. VA Enterprise Architecture Compliance

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

* 1. **VA Internet and Intranet Standards**

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

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1056&FType=2>

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): <https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1055&FType=2>

1. Physical Security & Safety Requirements:

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

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

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

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

1. The Contractor will have access to some privileged and confidential materials of VA.  These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA.  Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38.  Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information.  Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities.  Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract.  Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature.  If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information.  Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives.  The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
8. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
9. Controlled access to system and security software and documentation.
10. Recording, monitoring, and control of passwords and privileges.
11. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
12. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
13. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
14. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
15. Contractor does not require access to classified data.
16. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements.  All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none.  The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
17. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed.  In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

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

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

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.

1. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS
   1. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
   2. 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.
   3. 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.
   4. 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.
   5. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor’s employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.
2. VA INFORMATION CUSTODIAL LANGUAGE
3. 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).
4. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor’s information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA’s sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
5. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.
6. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.
7. 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.
8. 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.
9. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Directive 1605.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
10. 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.
11. The Contractor/Subcontractor’s firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.
12. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
13. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above-mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
14. 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.
15. SECURITY INCIDENT INVESTIGATION
    1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.
    2. 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.
    3. 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.
    4. 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.
16. LIQUIDATED DAMAGES FOR DATA BREACH
    1. 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.
    2. 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.
    3. 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:
       3. date of occurrence;
       4. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
       5. Number of individuals affected or potentially affected;
       6. Names of individuals or groups affected or potentially affected;
       7. 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;
       8. Amount of time the data has been out of VA control;
       9. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
       10. Known misuses of data containing sensitive personal information, if any;
       11. Assessment of the potential harm to the affected individuals;
       12. Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
       13. 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.
    4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
       1. Notification;
       2. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
       3. Data breach analysis;
       4. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
       5. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
       6. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.
17. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all the 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.

1. TRAINING
2. 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:
3. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior, relating to access to VA information and information systems;
4. Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176), Information Security and Privacy Role – Based Training for IT Specialists (TMS 2.0 # VA 3197), and complete this required privacy and information security training annually;
5. 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 – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
6. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
7. 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.

# 