

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

Financial Services Center (FSC)

Financial Technology Services (FTS)

Software Development Support

Date: October 31, 2024

PWS Version Number: 4.0

Contents

[1.0 BACKGROUND 4](#_Toc177725201)

[2.0 APPLICABLE DOCUMENTS 5](#_Toc177725202)

[3.0 SCOPE OF WORK 8](#_Toc177725203)

[3.1 ORDER TYPE 8](#_Toc177725204)

[4.0 PERFORMANCE DETAILS 8](#_Toc177725205)

[4.1 PERFORMANCE PERIOD 8](#_Toc177725206)

[4.2 PLACE OF PERFORMANCE 9](#_Toc177725207)

[4.3 TRAVEL 10](#_Toc177725208)

[5.0 SPECIFIC TASKS AND DELIVERABLES 10](#_Toc177725209)

[5.1 PROGRAM MANAGEMENT 10](#_Toc177725210)

[5.1.1 STAFFING PLAN 10](#_Toc177725211)

[5.1.2 PROGRAM MANAGEMENT 11](#_Toc177725212)

[5.1.3 CONTRACTOR PROJECT MANAGEMENT PLAN 12](#_Toc177725213)

[5.1.4 INDIVIDUAL PROJECT REPORTING REQUIREMENTS 12](#_Toc177725214)

[5.1.5 TECHNICAL KICKOFF MEETING 13](#_Toc177725215)

[5.1.6 WEEKLY/MONTHLY MEETINGS AND QUARTERLY PERFORMANCE REVIEW 14](#_Toc177725216)

[5.1.7 TECHNICAL DEBT BACKLOG 16](#_Toc177725217)

[5.1.8 PROJECT MANAGEMENT 17](#_Toc177725218)

[5.1.9 CHANGE AND CONFIGURATION MANAGEMENT 17](#_Toc177725219)

[5.1.10 CENTER OF EXCELLENCE (COE) SUPPORT 18](#_Toc177725220)

[5.1.11 CONTRACTOR PERSONNEL REQUIREMENTS 19](#_Toc177725221)

[5.2 RESEARCH AND ASSESSMENT, SYSTEM CONFIGURATION AND DEVELOPMENT AND TECHNICAL SUPPORT (T&M) 19](#_Toc177725222)

[5.2.1 RESEARCH AND ASSESSMENT SUPPORT 19](#_Toc177725223)

[5.2.2 DEVELOPMENT GUIDELINES AND TECHNICAL SERVICES 20](#_Toc177725224)

[5.2.3 SOFTWARE DEVELOPMENT AND DEPLOYMENT 21](#_Toc177725225)

[5.2.4 ADDITIONAL REQUIREMENTS 31](#_Toc177725226)

[5.2.5 ADDITIONAL CENTER OF EXCELLENCE (COE) SUPPORT 34](#_Toc177725227)

[5.3 TIER 3 SUSTAINMENT, PRODUCTION AND ANALYTICAL SUPPORT (T&M) 34](#_Toc177725228)

[5.3.1 SYSTEM AND APPLICATION SUSTAINMENT 35](#_Toc177725229)

[5.4 OPTIONAL TASK ONE: TRAINING 36](#_Toc177725230)

[5.5 OPTIONAL TASK TWO: TRANSITION SUPPORT 36](#_Toc177725231)

[5.6 OPTIONAL TASK THREE: ADDITIONAL PROJECT DEVELOPMENT 37](#_Toc177725232)

[6.0 GENERAL REQUIREMENTS 38](#_Toc177725233)

[6.1 ENTERPRISE AND IT FRAMEWORK 38](#_Toc177725234)

[6.1.1 VA TECHNICAL REFERENCE MODEL 38](#_Toc177725235)

[6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 38](#_Toc177725236)

[6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6) 40](#_Toc177725237)

[6.1.4 TRUSTED INTERNET CONNECTION (TIC) 40](#_Toc177725238)

[6.1.5 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM) 40](#_Toc177725239)

[6.1.6 FSC DEFINED PROCESS 41](#_Toc177725240)

[6.1.7 AUTHORITATIVE DATA SOURCES 41](#_Toc177725241)

[6.1.8 SOCIAL SECURITY NUMBER (SSN) REDUCTION 42](#_Toc177725242)

[6.2 SECURITY AND PRIVACY REQUIREMENTS 42](#_Toc177725243)

[6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 42](#_Toc177725244)

[6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 43](#_Toc177725245)

[6.2.3 Physical Security & Safety REQUIREMENTS 45](#_Toc177725246)

[6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 48](#_Toc177725247)

[6.4 PERFORMANCE METRICS 48](#_Toc177725248)

[6.5 FACILITY/RESOURCE PROVISIONS 50](#_Toc177725249)

[6.6 GOVERNEMENT FURNISHED PROPERTY 51](#_Toc177725250)

[6.7 RECORDS MANAGEMENT OBLIGATIONS 52](#_Toc177725251)

[ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 56](#_Toc177725252)

[ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 62](#_Toc177725253)

# BACKGROUND

The mission of the Department of Veterans Affairs (VA), Financial Services Center (FSC) is to provide high-quality financial services, exceeding the expectations of our federal customers, inspiring their trust and empowering them to focus on their core missions. The VA FSC Financial Technology Service (FTS) mission is to provide high- quality Information Technology (IT) infrastructure, software engineering, Electronic Commerce, and system support services to the FSC in accordance with the FSC's overall mission. In meeting these goals, VA FSC strives to provide high-quality financial services, exceeding the expectations of our federal customers, inspiring trust and empowering them to focus on their core missions.

The VA 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. In 2006, 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. VA FSC provides IT services in support of various initiatives throughout the FSC and VA.

The objective of this acquisition is to acquire IT Software Development Services to include software engineering and development, and developer and architect expertise to perform system development life cycle (SDLC) tasks in the development and support of applications and systems. Some of the applications developed to support the VA- FSC initiatives were developed utilizing Microsoft .NET, Pega PRPC, MS SQL Server, COBOL (mainframe-based), SNYCSORT (mainframe-based), Oracle, BPEL, and Java components. VA-FSC also provides Software Development Services in support of various initiatives throughout the FSC, Other Government Agencies (OGA) and VA. Attachment B contains a sample of projects supported by FSC development teams in 2019. The listing of projects is meant to be illustrative in nature and is not meant to define the scope that will be performed for this task order (TO).

The Government’s objectives are to:

1. Reduce operational costs
2. Enhance Government operations, particularly in development and support of applications
3. Seek consistency with Development maximum extent practicable.
4. Allow flexibility in meeting variable demands
5. Improve Government operations, particularly accountability and performance reporting
6. Provide procedural checks and feedback to improve compliance and management control on processes
7. Keep abreast of required technologies, standards and methodologies and propose to the FSC how to stay current with new versions of technologies as well as legislative mandates and other items as they relate to this TO

# APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541-3549, “Federal Information Security Management Act (FISMA) of 2002”
2. “Federal Information Security Modernization Act of 2014”
3. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules”
4. FIPS Pub 199. “Standards for Security Categorization of Federal Information and Information Systems,” February 2004
5. FIPS Pub 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006
6. FIPS Pub 201-2, “Personal Identity Verification of Federal Employees and Contractors,” August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
9. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
10. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
11. VA Directive 0710, “Personnel Security and Suitability Program,” June 4, 2010, <https://www.va.gov/vapubs/index.cfm>
12. VA Handbook 0710, “Personnel Security and Suitability Program,” May 2, 2016, <https://www.va.gov/vapubs/index.cfm>
13. VA Directive and Handbook 6102, “Internet/Intranet Services,” August 5, 2019
14. 36 C.F.R. Part 1194 “Information and Communication Technology Standards and Guidelines,” January 18, 2017
15. Office of Management and Budget (OMB) Circular A-130, “Managing Federal Information as a Strategic Resource,” July 28, 2016
16. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
17. NIST SP 800-66 Rev. 1, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,” October 2008
18. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended, January 18, 2017
19. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
20. VA Directive 6500, “VA Cybersecurity Program,” February 24, 2021
21. VA Handbook 6500, “Risk Management Framework for VA Information Systems VA Information Security Program,” February 24, 2021
22. VA Handbook 6500.2, “Management of Breaches Involving Sensitive Personal Information (SPI),” March 12, 2019
23. VA Handbook 6500.5, “Incorporating Security and Privacy into the System Development Lifecycle,” March 22, 2010
24. VA Handbook 6500.6, “Contract Security,” March 12, 2010
25. VA Handbook 6500.8, “Information System Contingency Planning,” April 6, 2011
26. VA Handbook 6500.10, “Mobile Device Security Policy,” February 15, 2018
27. VA Handbook 6500.11, “VA Firewall Configuration,” August 22, 2017
28. 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>
29. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)
30. VA Directive 6508, “Implementation of Privacy Threshold Analysis and Privacy Impact Assessment,” October 15, 2014
31. VA Handbook 6508.1, “Procedures for Privacy Threshold Analysis and Privacy Impact Assessment,” July 30, 2015
32. VA Handbook 6510, “VA Identity and Access Management,” January 15, 2016
33. VA Directive and Handbook 6513, “Secure External Connections,” October 12, 2017
34. VA Directive 6300, “Records and Information Management,” September 21, 2018
35. VA Handbook, 6300.1, “Records Management Procedures,“ March 24, 2010
36. 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
37. 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)
38. VA Directive 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” October 26, 2015
39. VA Handbook 0735, “Homeland Security Presidential Directive 12 (HSPD-12) Program,” March 24, 2014
40. 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
41. OMB Memorandum M-19-17, “Enabling Mission Delivery Through Improved Identity, Credential, and Access Management,” May 21, 2019
42. OMB Memorandum, “Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation,” May 23, 2008
43. 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>)
44. NIST SP 800-116 Rev 1, “Guidelines for the Use of Personal Identity Verification (PIV) Credentials in Facility Access,“ June 2018
45. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, “Digital Identity Guidelines,” updated March 02, 2020
46. NIST SP 800-157, “Guidelines for Derived PIV Credentials,” December 2014
47. NIST SP 800-164, “Guidelines on Hardware-Rooted Security in Mobile Devices (Draft),” October 2012
48. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981, “Mobile, PIV, and Authentication,” March 2014
49. 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>)
50. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514>)
51. VA Memorandum “Personal Identity Verification (PIV) Logical Access Policy Clarification,” July 17, 2019, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4896>
52. Trusted Internet Connections (TIC) 3.0 Core Guidance Documents, <https://www.cisa.gov/publication/tic-30-core-guidance-documents>
53. OMB Memorandum M-19-26, “Update to the Trusted Internet Connections (TIC) Initiative,” September 12, 2019
54. OMB Memorandum M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure,” August 22, 2008
55. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
56. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
57. Executive Order 13834, “Efficient Federal Operations,” dated May 17, 2018
58. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
59. VA Directive 0058, “VA Green Purchasing Program,” July 19, 2013
60. VA Handbook 0058, “VA Green Purchasing Program,” July 19, 2013
61. Office of Information Security (OIS) VAIQ #7424808 Memorandum, “Remote Access,” January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
62. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
63. “Veteran Focused Integration Process (VIP) Guide 4.0,” January 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
64. VA Memorandum “Proper Use of Email and Other Messaging Services,” January 2, 2018, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28>
65. “DevSecOps Product Line Management Playbook” version 2.0, May 2021, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4946>
66. NIST SP 500-267B Revision 1, “USGv6 Profile,” November 2020
67. OMB Memorandum M-21-07, “Completing the Transition to Internet Protocol Version 6 (IPv6),” November 19, 2020
68. Social Security Number (SSN) Fraud Prevention Act of 2017

Section 240 of the Consolidated Appropriations Act (CAA) 2018, March 23, 2018

# SCOPE OF WORK

The Contractor shall provide project management, research and assessment, development guidelines, technical services, software development and deployment support to the FSC including software engineering, software development, and system solution architect expertise to perform system development life cycle (SDLC) tasks in the development of applications and systems. The Contractor shall provide tier 3 system sustainment support, production and analytical support for all FSC solutions. The Contractor shall provide Center of Excellence support as well as optional mentoring and training. The Contractor shall follow a scaled Agile Methodology such as SAFe and the VIP software development lifecycle established by VA’s Office of Information and Technology (OI&T) Enterprise Program Management Office (EPMO). Change made by VA OIT to VIP and VA implementation of agile development shall be adopted by the contractor. The Contractor shall provide system and application sustainment support for the FSC’s portfolio and features.

The Contractor shall execute the work described above, provide the necessary processes, manage its staff, and develop processes and procedures to improve the FSC’s maturity in the development and maintenance of software systems.

## ORDER TYPE

The effort shall be proposed on a Firm Fixed Price (FFP) basis.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a 12-month base period with four (4) 12-month option periods, if exercised. Additional support may be included via two (2) optional tasks.

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, four 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 located in the main FSC offices at 8000 Metropolis Drive, Bldg B., Austin, TX 78744 AITC 1615 Woodward Street, Austin Texas 78741, and other local satellite offices within Austin, Texas. Work may be performed at remote locations with prior concurrence from the Contracting Officer’s Representative (COR).

Contractor employees may work off site on a case-by-case basis, with the approval of the COR and/or CO. A Contractor employee may be required by the Government to attend face to face meetings at the main FSC office at no cost to the Government for travel. There shall be no additional cost to the Government for remote workers in terms of travel or labor rates. The Contractor shall identify the Contractor’s place of performance in their proposal submission.

## 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.  Travel expenses will be on a Firm-Fixed-Price basis.

The Contractor shall provide a Trip Report which shall include the following:

* Meeting purpose and scope
* FSC attendees
* Meeting topics
* Detailed notes on topics that are of importance to FSC
* Action items

The Trip Report shall be submitted within 3 calendar days of completion of travel.

The estimated number of trips in support of program related meetings for this effort are up to ten (10) events per year. Examples of travel include but are not limited to the following:

1. One (1) representative to attend three (3) X12 Standing meeting per year (See http://x12.org/x12org/meetings/x12trimt/asc-x12-standing-meetings.cfm)
2. Two (2) representatives to attend one PEGAWorld event per year (see <https://www.pega.com/events/pegaworld>)
3. One (1) representative to attend a 3-day meeting with regarding EHRM effort

**Deliverable:**

1. Trip Report

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall perform the following:

## PROGRAM MANAGEMENT

### STAFFING PLAN

The Contractor is required to provide a sufficient quantity of skilled staff sufficient to perform all of the tasks described within this PWS. The Contractor shall provide a Staffing Plan within 10 calendar days after TO award. The Contractor shall provide a mixture of developer skill levels including but not limited to Junior, Senior and Expert Developers, and Software/System architects. The Staffing Plan will reflect SAFe Agile methodology and industry best practice. The Government shall provide the Contractor information on future changes for development services as soon as practical and confirm as part of the quarterly reviews (see 5.1.6) so that the Contractor may proactively plan adjustments to the Staffing Plan.

The Key Technologies critical to the success of Software Development at the FSC include, but are not limited to, PEGA, Electronic Data Interchange (EDI), Java, and .NET. The Contractor shall identify as key personnel within the staffing plan the lead software / system architects by name to support PEGA, EDI, .NET and Java who will provide expert support to developers across scrum teams within their assigned technologies. Support will include but not be limited to:

1. Establishing and recommending best practices
2. Executing code peer reviews
3. Resolving complex technical issues including defects
4. Aligning solutions with enterprise design patterns
5. Validating security controls have been integrated
6. Implementing and improving upon existing DevSecOps process
7. Verifying that all system documentation is complete and accurate

Normally, scrum teams will include two (2) full time developers but can be up to four (4) developers or one (1) full time developer and a backup resource.

The Staffing Plan will assume FSC office hours are 6AM to 6PM central time Monday to Friday. The Staffing Plan shall include means for working outside normal business hours.

The Staffing Plan shall include administrative staff, management staff, and other resources, such as specialist and subject matter experts, necessary to meet the requirements of the PWS. Any change to staff levels or availability which could impact sprint velocity shall be reported to the government as soon as practical but a minimum of two (2) business days in advance of any realignment.

**Deliverable**:

1. Staffing Plan

### PROGRAM MANAGEMENT

The Contractor shall identify an onsite Program Manager (PM) by name, who shall provide management, direction, administration, quality assurance, and leadership of the execution of this PWS. The PM shall ensure all Contractor personnel are appropriately qualified to perform on this TO. The Contractor’s PM shall provide day-to-day program management guidance and direction to Contractor personnel in the execution of tasks defined in this PWS.

The Contractor shall use VA approved project management and software development methodologies and toolsets, such as VIP that assure that all contract-driven activities are identified, documented, and tracked so that the contract shall continuously be evaluated and monitored for timely and quality service. The Contractor shall notify the FSC COR of any technical, financial, personnel, or general managerial problems encountered throughout the PoP. The Contractor shall migrate to new or revised development methodologies and toolsets as they are approved by the Government.

The Contractor shall input their actual work hours by activity into the VA-FSC’s Activity Based Costing (ABC) Labor Tracking each Government Pay Period or other similar tracking tool designated by FSC. Users have up to the Tuesday following the end of the Pay Period to enter their time in the Portal. Pay Periods close automatically midnight on Wednesdays.

### CONTRACTOR PROJECT MANAGEMENT PLAN

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

The Contractor shall deliver a draft CPMP at the kickoff meeting. A final CPMP is due 10 calendar days after the kickoff meeting. Quarterly updates shall be reviewed at the Quarterly Performance Management Review (QPMR) meeting. At a minimum, the CPMP shall include the following:

1. Organizational Chart
2. Roles and Responsibilities document
3. Transition Plan (IN) and timeline
4. Staffing Plan and timeline

**Deliverable:**

A. Contractor Project Management Plan

### INDIVIDUAL PROJECT REPORTING REQUIREMENTS

The Contractor shall continuously monitor project-level activities and shall provide, upon request, input to the FSC PM and/or COR on the following topics:

1. Risk management
2. Requirements definition and management
3. Configuration management
4. Test management
5. Quality control
6. Technical compliance

In addition, the Contractor shall perform the following reporting activities:

1. Provide accurate estimate of duration and/or effort for tasks assigned to contractor’s staff within a given timeframe, normally by end of a specified sprint. Estimate to be recorded in Agility or other government approved product management tool.
2. Weekly report providing status on in-progress work during scrum sessions or other team meetings.
3. Ensure that development tasks have been assigned to qualified staff. Task assignments will be recorded in Agility or other government approved product management tool.
4. Document commitments from development team to complete specified tasks within a given timeframe, normally by end of a specified sprint.
5. Weekly report that shows product team performance relating to level-of-effort, schedule, and release cadence.

The Weekly Status Report is due the first business day of the week by noon central time. Deliveries of this report shall begin within 14 calendar days of contract award.

The Weekly Product Team Performance Report is due the first business day of the week by noon central time. Deliveries of this report shall begin within 14 calendar days of contract award.

**Deliverables:**

A. Weekly Status Report

B. Weekly Product Team Performance Report

### TECHNICAL KICKOFF MEETING

A technical kickoff meeting shall be held within 10 calendar 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 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 FSC Software Development Services Task Order.” The Contractor shall submit the final updated kickoff meeting presentation to the CO for review and signature within 3 calendar days after the meeting. The Contractor shall prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR and all attendees within 3 calendar days after the meeting.

**Deliverable:**

* + - 1. Technical Kickoff Meeting Agenda
      2. Final Technical Kickoff Meeting Presentation
      3. Final Technical Kickoff Meeting Minutes

### WEEKLY/MONTHLY MEETINGS AND QUARTERLY PERFORMANCE REVIEW

The Contractor shall participate in routine and ad hoc status meetings and VA Quality Reviews (i.e., Functional Reviews). The VA Quality Reviews meeting schedule will be defined upon delivery of the project schedule from the CPMP.

The Contractor shall provide a Weekly Progress Report (WPR) which covers all work completed during the reporting period and work planned for the subsequent reporting period. The WPR shall cover schedule, action items, risks, and issues for three areas of work: projects, production support, and division action items. The WPR can be a single report or broken up into multiple reports. The exact format of the report shall be suggested by the Contractor and approved by the Government. The Contractor may deploy a dashboard as an alternative to a static report. The WPR will be delivered on the first business day of the week by noon central time. Deliveries of the WPR should begin within 14 calendar days of contract award.

Developer staff shall enter data as required into Agility or other government approved product management tool. Contractors shall support the creation of a weekly status report in consultation with other stakeholders.

Production Support: At a minimum, the WPR shall contain the following data elements for production support:

1. Number of open production support tickets assigned to development staff including work that was uncovered during the warranty phase of the project.
2. Resolution time/metrics.
3. Total hours spent on all production support tasks by program.

The Contractor shall keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

The Contractor shall also coordinate with VA FSC team management or coordinators and other key Government personnel for additional progress reviews to relay software development progress and address any issues or concerns as needed.

The Contractor shall convene a monthly Program Development Activity and In-Progress Review (IPR) Meeting with the COR, and other key Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed, monthly, of the analysis and documentation efforts underway to ensure that management oversight, policy, procedures, contract management, budgets and other development activities are properly coordinated, and remain on budget. The meetings will provide the opportunity for Government and Contractor personnel to discuss SOPs, interpretation of VA regulatory guidance, and other mission-critical activities. The meeting will provide opportunities to identify other activities, establish priorities, and coordinate resolution of identified problems or opportunities. The IPR will be held the first full calendar week of the month and the Program Development Activity report is due 5 calendar days before the IPR meeting. At a minimum, the Contractor shall report on the following division items as part of the monthly Program Development Activity report:

1. Number of staff onboarded by skill set, experience level, and role
2. Number of unfilled positions that are being recruited
3. Total number of project hours consumed by each program by fiscal year to date, and calendar year to date
4. Status on action items
5. Staff members’ current scrum teams' assignment(s). If staff member is assigned to multiple scrum teams, then report is to indicate which assignment is considered the most important.

The contractor shall perform Quarterly Performance Management Reviews (QPMRs) within 5 business days of the end of the quarter. The contractor shall provide a Quarterly Status Report 7 business days prior to each QPMR. The Quarterly Status Report shall address the status of projects progress, schedule, risks, any issues encountered, and shall address any updates made to the CPMP. The Contractor shall conduct QPMRs to discuss and provide in-depth information on the subjects addressed in the Quarterly Status Report. The Contractor shall update the Quarterly Status Report to capture the meeting minutes of each QPMR. The meeting minutes should, at minimum, reflect members in attendance at the QPMR and capture issues discussed, decisions made, and action items assigned. The updated Quarterly Status Report is due 5 business days following the QPMR.

The Contractor shall attend meetings such as change control, scrums, scrum of scrums, and project status meetings to monitor, track, and provide status updates on the project schedule.

Weekly, monthly, and quarterly reports shall be submitted in electronic form in Microsoft Word or other approved formats.

**Deliverables:**

1. Weekly Progress Report
2. Monthly Program Development Activity Report
3. Quarterly Status Report

### TECHNICAL DEBT BACKLOG

The Contractor shall participate in identifying non-functional requirements related to compliance (Section 508, security, technical standards), technical roadmap, enterprise services, technical refresh, and any known technical gaps for existing products collectively known as technical debt.

The Contractor shall execute requirements reviews with IT and Business stakeholders to capture, review, clarify, and prioritize non-functional epics and user stories regarding technical debt. The Contractor shall create enterprise level epics and user stories which are then applied to multiple products within FSC.

The Contractor shall coordinate with the FSC Project Manager, the Product Owner, and the FSC Configuration Management representative to incorporate Technical Debt Backlog requirements into the appropriate product backlogs, build plans, and sprint plans. These technical debt items may be worked as part of larger projects, or the Government may assign them to projects limited to technical debt items.

Every six (6) months, the Contractor shall conduct a technical review to determine if new non- functional requirements have been created that must be included in the technical debt backlog. Sources of new non-functional items include, but are not limited to, the following:

1. Directives from VA OIT
2. Revisions to the VA Technical Reference Model (TRM)
3. Regulatory changes which impact VA system

The Contractor shall support the following changes as needed to support FSC’s Authority to Operate (ATO) review cycle:

1. Perform static code review and remediate critical, high, and medium findings. Low findings are to be placed in product backlog
2. Perform information assurance review and remediate critical, high, and medium findings. Low findings are to be placed in product backlog
3. Update system documents included in the Authority to Operation (ATO)
4. Update code to most recent version or framework
5. Validate code trunk matches production
6. Validate that all databases are under source control
7. Review and update system documents including Software Design Document (SWDD) and data dictionary
8. Review and update production support documents including the Product Operations Manual (POM)

### PROJECT MANAGEMENT

The Contractor shall provide the following Project Management services:

1. Provide a single POC for schedule packages, schedule status updates, resource assignments, problems, issues, and escalations.
2. Coordinate all Contractor development activities.
3. Develop and provide research, decision, and recommendation papers regarding current and future Division operations.
4. Provide short and long-term planning guidance and support in support of Contractor staff and coordinate with FSC project stakeholders.
5. Provide support to FTS supervisors and Division Chiefs on all areas of Division operations, SDLC, research, and special projects.
6. Provide briefings and management reports on as needed basis (i.e., weekly, monthly, and quarterly).
7. Ensure coordination of efforts with other sections within the FSC especially the PMO, FTS Operations and Maintenance Division and FSC Enterprise Architecture.
8. Ensure that all development tasks are completed on time and that accurate and timely status is given to the FSC PM.
9. Coordinate development activities such as meetings, document reviews, creating schedule packages, and ensure adequate planning and closeout activities are accomplished.
10. Ensure the development team is communicating and coordinating effectively with other project stakeholders.

The Contractor shall remain flexible to organize development resources differently as needed to support the development projects under this effort.

### CHANGE AND CONFIGURATION MANAGEMENT

The Contractor shall ensure staff follow and improve upon the existing DevSecOps process for change and configuration management. The Contractor shall support FSC Configuration Management and Change Management activities within a Cloud and on-premises environment. The Contractor shall:

1. Conduct quality reviews of all documentation before submitting them to the Government.
2. Maintain current versions of all source code. Source code shall be checked in daily into the FSC source code repository. Maintain source code in designated escrow.
3. Improve the existing DevSecOps solution which enables the continuous integration and deployment of code.
4. Follow VA FSC change and configuration management procedures during each phase of the SDLC.
5. Adhere to VA FSC software development and documentation standards.
6. Provide documentation to ensure future developers and administrators can easily understand the code logic, application usage, and implementation.
7. Provide input on the Configuration Management plan for software configuration processes and procedures related to development, integration, testing and fielding systems.
8. Provide input on appropriate standards of documentation and management control for promotion of software releases from one environment to another.
9. Update the Technical Documentation Package as required to reflect change and configuration management activities.

### CENTER OF EXCELLENCE (COE) SUPPORT

The Contractor shall support six (6) SAFe Agile, .NET, Electronic Data Interchange (EDI), Enterprise, DevSecOps, and Pega centers of excellence to provide technical oversight related to the Development and Electronic Commerce Division’s key technology platforms.

The Contractor shall:

1. Provide expert support to the Government on the key technologies including industry best practices and technology trends.
2. Set technology standards for design, coding, and testing for the Key Technologies. The Contractor shall also track and enforce compliance with the technology standards.
3. Be the technical expert to support FTS leadership in communication with vendors and external partners on topics of development platforms.
4. Develop, document, maintain, and enforce .NET, BPEL and Pega Development standards, as well as other standards required for VA use across all FSC products, programs, and projects.
5. Support Enterprise Architecture roadmap by providing technical refresh recommendations.
6. Track new versions of the development platforms and recommend an upgrade schedule to the Government.
7. Identify development training needs related to the development platforms.
8. Maintain Pega and other industry certifications
9. Be the technical liaison to the appropriate vendor. For instance, the Pega Center of Excellence shall be the technical liaison between the Government and Pega Inc.
10. Coordinate and collaborate with other designated personnel assigned to the COE.
11. Provide hands on keyboard support when necessary to resolve complex issues and/or short-term surge capacity.

### CONTRACTOR PERSONNEL REQUIREMENTS

The Contractor shall provide program and project manager points of contact who shall be responsible for the performance of the work and work team. The name of these people and an alternate who shall act for the Contractor when the manager is absent shall be designated in writing to the COR. The Contractor’s program and project manager or alternate shall have full authority to act for the Contractor on all contract matters relating to daily operation of this task order.

The Contractor shall provide continuous and uninterrupted support throughout the period of performance. The Contractor shall be responsible for managing its personnel to ensure there are no disruptions in the level or quality of services even if its personnel are unavailable for any reason including vacations, illnesses or terminations.

## RESEARCH AND ASSESSMENT, SYSTEM CONFIGURATION AND DEVELOPMENT AND TECHNICAL SUPPORT (T&M)

FSC receives development projects for financial and healthcare systems from VA and other Government agencies throughout the year. The scope and technical requirements of each development effort are unknown in advance. Therefore, FSC needs an agile workforce capable of supporting developing efforts using FSC’s current key technologies and adopting new technology as the IT industry evolves. For each development effort, the Contractor shall follow the VIP Agile development approach outlined below.

### RESEARCH AND ASSESSMENT SUPPORT

The Contractor shall provide research and support for the Government’s assessments of future industry system architecture, software development direction, emerging trends, best practices, automated tools, innovative approaches, and contribute, when appropriate, on development issues and technology assessments. The Contractor shall use information obtained from this research to assist FSC leadership in defining and shaping roles, responsibilities, vision, goals, and objectives for development, systems and application sustainment or maintenance, and analysis. The Contractor shall also provide research results with respect to SDLC tools and best practices from private industry. The Contractor shall be prepared to present research findings and recommendations during monthly IPRs, or in written form to include point papers or articles for publication.

### DEVELOPMENT GUIDELINES AND TECHNICAL SERVICES

As a Federal Acquisitions Academy Program/Project Management organization, the FSC FTS follows the VIP software development methodology with which the Contractor must adhere.

Under the VIP software development methodology, the acceptable project management methodologies fall under DevSecOps, Agile, Test-Driven Development (TDD) and Agile

SCRUM. The Government will inform the Contractor of any changes to the software development methodology.

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

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

The Contractor shall support Information Technology Infrastructure Library (ITIL) Tier 3 production control processes (particularly incident management and problem management) required to identify problems and provide prompt resolution as needed.

Although primarily focused on the development phase of the SDLC, the Contractor shall be a stakeholder in all phases and play a key role in the planning phase of the project. The Contractor shall elaborate and manage non-functional requirements and complete design activities. The Contractor shall provide SDLC expertise, process and tool recommendations related to the scope of the PWS. Additionally, the Contractor shall coordinate with other SDLC stakeholders, such as the PMO, on process improvements.

The Contractor shall contribute to the tailoring of SDLC processes and tools for the FSC. These tailored SDLC processes will describe the management for all processes, practices, and methods under which the VA FSC systems are designed, developed, tested, integrated, documented, and maintained. Any updates to the FSC SDLC and SDLC processes shall be reviewed by all impacted stakeholders and approved by the Government. The FSC SDLC updates and SDLC processes are owned by the Government. The Contractor shall propose process improvements based on lessons learned to the process improvement team or other group designated by the Government. FSC SDLC updates and SDLC processes include, but are not limited to, the following:

1. Tailoring VA SDLC to improve efficiency of delivery in accordance with VA’s VIP methodology.
2. Improving existing processes, procedures, and methods in support of the SDLC within the Contractor’s scope of activities such as technical design or code reviews.
3. Assuring all resources are trained on and use the SDLC and supporting processes, procedures, tools, templates, and methods.
4. Incorporating new tools to facilitate the use of the SDLC, such as specific document templates and automated tools.
5. Enhancing existing software development best practices, such as source code management, enterprise data management, build and deployment, adoption of new software development approaches and maintaining currency with advances specifically in the Healthcare and Financial sectors.

The current VIP SDLC is the starting point for any SDLC updates and is the foundation for the FSC SDLC processes. The FSC SDLC is continually reviewed and updated. See attachment A for summary of the VIP SDLC.

### SOFTWARE DEVELOPMENT AND DEPLOYMENT

The Contractor shall provide software development and deployment support to (a) develop, test, and deploy FSC applications and (b) customize existing applications following the approved SDLC and required tasks below:

#### AGILE REQUIREMENTS ELABORATION AND DESIGN

The Contractor shall review and elaborate on the derived technical requirements of the solution. The Contractor shall propose non-functional requirements from the technical debt backlog for inclusion in builds with an emphasis on those items where the Government would realize savings by integrating functional and non-functional requirements into a single build. The Contractor shall provide recommendations to the FSC PM on prioritization of non-functional requirements. The Contractor shall inform the PM of any nonfunctional requirement that must be completed prior to the next production release of the solution such as resolving security findings.

The Contractor shall:

1. Participate in elaboration sessions with the FSC PMO, external partners, and customer representatives to finalize functional requirements.
2. Ensure that the information collected (epics, user stories, acceptance criteria and data exchange requirements) is sufficient to deliver the necessary system or application functionality. This includes the ability to translate requirements into terms that can be implemented in system designs.
3. Complete systems analysis for all components of systems or applications, working in close coordination with other project team members to assure effective and efficient systems component integration and address system dependencies.
4. Elaborate and maintain compliance (Section 508, security, technical standards) requirements in the form of Epics and User Stories to ensure that all Contractor-produced or supported applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration, VA 508 guidelines, VA NIST 6500, and the common security configuration guidelines provided by NIST, VA and any other Federal Agency as required by VA or Federal Regulations.
5. Coordinate with project teams to integrate non-functional requirements into the product backlog and establish build and sprint plans that incorporate both functional and non- functional features.
6. Establish initial Unit of measurement (e.g., Story Points) as the estimated relative complexity of user stories.
7. Identify the development and test environment access that is needed for developers no later than five (5) days after the completion of the design. Access requests for new environments will be submitted within five (5) days of identification and at least three (3) days prior to development start.

All technical epics, features, visualizations, user stories, and other sources of requirements information for non-functional requirements shall be input and maintained in Agility or a similar solution specified by the Government. All requirements data is under change control and shall be fully linked to work items that show traceability to design changes, configurable items, test cases and test results.

**DESIGN**

The Contractor shall apply Solution Architect expertise to develop the appropriate architectures for each project. The Contractor shall abide by standards established by the Enterprise Architecture group. Architecture is started during the planning phases and refined during the project builds. The Contractor shall deliver incremental deliveries of the architecture documentation during the project builds and deliver the final documentation by the end of the project.

The Contractor shall:

1. Elicit business requirements and translate those requirements into technical solutions that may include one or more of the following: Commercial off the Shelf (COTS), Service Oriented Architecture (SOA) components, custom-developed software, EDI, and interfaces.
2. Utilize SOA and microservice principles such as standardized service contracts, service loose coupling, service abstraction, service reusability, service autonomy, service statelessness, service discoverability, service composability, and service scalability.
3. Coordinate system and application designs with the rest of the project stakeholders.
4. Provide software architecture documents to establish a blueprint for the design, including specifications for hardware, software, people, interfaces, integrations, and data resources.
5. Trace Architecture components to functional requirements.
6. Support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One- VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap.
7. Validate that the implementation matches the system architecture blueprint during testing.
8. Provide expertise to the rest of the project stakeholders on the solution design and implementation.
9. Utilize Enterprise Standards from the FSC’s Enterprise Architecture (EA) team and provide input into EA standards.
10. Coordinate system and application designs with the FSC EA group and external entities such as other VA organizations (e.g., OI&T Enterprise Operations (EO)).
11. Contribute to the Interface Control Document (ICD) to describe the interface specification for all external interfaces.
12. Create initial Software Design Document (SWDD) to capture detailed solution design prior to increment planning. Maintain and revise the SWDD during the development cycle as additional information regarding actual implementation becomes known.
13. Participate in a Preliminary Design Review (PDR) with enterprise architecture team and the project team prior to Critical Decision #1 and a Final Design Review (FDR) prior to Critical Decision #2. The PDR is a meeting to review and get Government approval for the initial solution design. The FDR is a meeting to review any changes to the solution design that were made during development. These design reviews ensure the documentation is current, under configuration management, communicated to the project team, and approved by the Government.
14. Design BI solutions currently using the Agile project management methodology. Analytics BI solutions and products include but are not limited to advanced visual analytics dashboards, paginated reports, customized analytics applications and/or power apps, etc. to provide modernized reporting capabilities.
15. Provide design and architecture support for the development of data base management, data management systems.
16. Design IT software solutions that solve the problems related to adequate use of data to ensure optimal business outcomes. Methods used for designing and architecting solutions will include but not limited to database diagrams and documentation using expertise within the enterprise systems data models and processes.
17. Find new ways of supporting business intelligence and decision making.
18. Design logical and physical data models according to business requirements.
19. Define the data requirements and structure for the application.
20. Model and design the application data structure, storage, and integration.
21. Understand current Client data landscape and define target state data architecture.
22. Provide guidance on industry standard data models with respect to the Client target state data architecture and strategy.
23. Document the target state conceptual and logic data models.
24. Design to implement solutions in various technologies like (but not limited to) Data warehousing, Databricks and big data. SQL, Power BI, AWS, cloud technology, containerization, SSRS/SSIS, decision support systems, Enterprise data management, and modern data architecture best practices.
25. Provide Business Data Architecture support to fully utilize and maintain data estate, on-premises, and/or cloud environments required to maximize functionality for BI solutions.

The Contractor shall contribute to the Technical Documentation Package of each project and provide input for each item below, if applicable, to the specific effort and update to reflect any changes as they occur. Note that this list may change based on the most current version of the VIP required documents or using a tailored version of the artifact approved by the FSC. Requirements and approval processes for each document will be specified in the related SOP and/or within the document itself.

1. Architecture diagrams including traceability Matrix (Owned by FSC Enterprise Architecture Unit Test Cases and Results)
2. Security Vulnerabilities Report (Owned by Information Assurance)
3. Interface Control Documents (Owned by Business Analyst/Business Architect)
4. Production Operations Manual (POM) (Initial POM is owned by Project manager. POM for existing applications is owned by operations team)
5. Project schedule packages for Development (Owned by scheduler or scrum master)

For each project, the Contractor shall be responsible for the following items within the Technical Documentation Package. Note that this list may change based on the most current version of the VIP document. These

1. Cumulative Release Notes
2. Deployment and Installation Guide
3. Deployment, Installation, Rollback, Back-out Guide

The following items are deliverables under PWS Section 5.2.3.1: SWDD, Cumulative Release Notes, Deployment and Installation Guide, and Deployment, Installation, Rollback, Back-out guide. Each of these deliverables are due no later than 5 calendar days prior to submission to the Change Control Board (CCB) for approval.

Deliverables:

1. Software Design Document (SWDD)
2. Cumulative Release Notes
3. Deployment and Installation Guide
4. Deployment, Installation, Rollback, Back-out Guide

#### BUILD/ PRODUCT INCREMENT PLANNING

The Contractor shall participate in build and/or product increment planning prior to the start of each build to assign items from the backlog to the build. The Contractor shall assist the project team in developing the Build Plan prior to Critical Decision #1 by estimating the user stories in the product backlog and providing recommendations for sequencing. Each build shall enable the team to promote solutions into the production environment at least once every 90 days unless a waiver is approved by FTS leadership.

The Contractor shall contribute to the creation of the Build Plan or the Increment Plan in collaboration with the project team prior to beginning the development cycle. The plan is the scope of work which will be completed in the agreed upon build timeframe. Each build or increment will have at least one new release or push to production. The Contractor shall follow the standard development cycle as outlined below in Section 5.2.3 and all subparagraphs for all builds.

A build or increment will typically consist of five two or three-week sprints, however the sprint length and number of sprints per build will be defined by the scrum team based on the needs of the project.

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

Prior to the start of development, the Contractor shall identify the resources assigned to development tasks within the sprint on the Staffing Plan. If necessary, the Contractor shall schedule meetings to address any concerns raised by the Government with the proposed scrum team(s). Whenever practical, the Contractor shall maintain continuity of scrum team(s) between builds to maximize institutional knowledge. If it is not possible to retain the continuity of a scrum team, the Contractor shall notify the Government of the change in scrum team.

Backlog grooming and prioritization are continued throughout the product life cycle and shall be managed throughout the period of performance. All activity scheduled in each build and

backlogs shall be captured and have status showing all work items, changes, impediments, and retrospectives. All data and artifacts in Team Concert or other project management tool shall be fully linked to requirements data and test data.

#### SPRINT PLANNING

Once the Build Plan is completed and accepted, the Contractor shall participate in Sprint Planning sessions. All activity scheduled in each sprint and backlog shall be captured and have status showing all work items, changes, impediments, and retrospectives. All data and artifacts shall be fully linked to requirements data and test data by the scrum team.

The Contractor shall:

1. Create development tasks for each user story and document them in Agility or any other government designated tool.
2. Establish unit of measurement (e.g., Story Points) as the estimated relative complexity of user stories.
3. Participate in a Sprint Planning Meeting, at the beginning of each sprint.
4. Commit to completing a mutually agreed set of tasks by the end of the sprint.

#### SPRINT EXECUTION

The Contractor shall capture all activity executed in each sprint and backlog and have status showing all work items, changes, risks, issues, impediments, and retrospectives. All data and artifacts shall be fully linked to requirements data and test data. All project artifacts and source code shall be under change and configuration management as specified by the COR using Agility or other tool specified by the government.

The Contractor shall:

1. Develop the features and capabilities as work items that were established in the Build and Sprint Plans and record in Agility or other tool as specified by the government
2. Complete sprint development including disciplined automated testing (unit, functional, regression) and reviews as a continuous process, to avoid finding issues at the end of sprint development.
3. Participate in scheduled scrum meetings (typically 15 minutes) to show the team progress, impediments and daily plans.
4. Update Agility or other designated project management tool daily, to include progress on tasks during sprints, blockers and dependencies.
5. Support demonstration of the sprint activities with the project team and users at the end of each sprint. This is termed a Sprint Review and will result in Customer Acceptance of the Sprint.
6. Develop and deliver automated build and automated publishing capabilities to schedule jobs and support continuous integration for every sprint. Automated build tools shall follow the approved list from the One-VA TRM (Technical Reference Model) and code shall be demonstrable and stable enough to be promoted to another environment without issue by evidence of the status of tests and results in the Agility or other government designated tools..
7. Participate in a Sprint Retrospective at the end of the Sprint to provide team performance lessons learned.
8. Support a stable development environment by executing automated tests after infrastructure changes per the change management policy.
9. At a minimum, the Contractor shall support the following technologies for FSC:
   * + Mulesoft
     + Java
     + Oracle Script
     + GitHub

Pega PRPC, Pega Government Platform, Pega Generative AI, Case Management, Robotics, and CPM

* + - Microsoft.NET
    - BPEL Digital.ai.AgilityMicrosoft SharePoint
    - OpenText TrustedLink Enterprise (TLE)
    - Cleo VL Trader
    - Microsoft SQL Server and Oracle database
    - Oracle WebLogic
    - IBM FileNet Content Manager
    - Mobile Development technologies
    - Microsoft Dynamics GP
    - Microsoft Customer Relationship Management (CRM)
    - TIBCO Spotfire
    - TIBCO Active Matrix – BPM
    - TIBCO Automation Services
    - SAS Base;
    - Tableau
    - Power Apps platform, including but not limited to PowerBI
    - Databricks
    - Other BI tools and technologies including but not limited to, Microstrategy, SAP business objects, SAP HANNA, and CFO Control Tower
    - Cloud technologies: Microsoft Azure/Amazon Web Services
    - Oracle Golden Gate
    - Data masking: Informatica and Asterix

1. Use industry standards in database management, data analytics and business intelligence for development of a wide range of analytic solutions and products
2. Develop and support development of solutions to derive insight and understanding from large data sets through data visualization, building informative reports / dashboards, application of statistical methods, and deep investigation. Provide advanced knowledge in using data visualization and drive action by presenting information, defining and designing dashboards / reports that summarize customer insights and highlight “hot spots” for the customer.
3. Work with Data Engineers, Data Architects, and Data Scientists, to help define back-end requirements for data products (aggregations, materialized views, tables – visualization), data investigation to discover correlations / trends and the ability to explain them, and collaborate with internal and external customers to develop an analytics portfolio consistent with the vision and goals of stakeholders.
4. Provide deep knowledge in SQL programming skills with an understanding of database capabilities. Expertise in and provision of visual solutions, such as Microsoft Power BI, as well development of analytic products using the full spectrum of descriptive, diagnostic, predictive, and prescriptive analytic methods.
5. Support 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 exploratory data analysis (EDA) in support of development of the analytic solution.
6. 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 BI platform in business-friendly and accessible ways.
7. Provide BI Service Offerings through the creation of simple to use, intuitive, robust, and accurate reports to provide integrated reporting solution and integrate statistical and quantitative models into the BI platform.

#### TESTING

The Contractor shall support testing conducted by the business, PMO, and any third-party testing including functional, user, regression, integration, performance, user interface, end to end, security and Section 508 compliance. The Contractor shall support triage meetings and remediation of defects.

The Contractor shall support Agile and TDD best practices for integration testing into each Agile development sprint and build. The Contractor shall conduct unit tests throughout the development phase using industry best practices of continuous integration methods and automated regression testing utilities using One-VA TRM approved tools.

The Contractor shall support the development and maintenance of an automated regression suite of unit tests that can be executed whenever there is a change to the system and/or infrastructure. The Contractor shall expand and improve on existing DevSecOps efforts to fully integrate automated testing with automated deployment across all environments.

The Contractor shall remediate defects uncovered during compliance testing for security and Section 508 accessibility requirements. The Contractor shall create and maintain internal coding standards which are designed to prevent duplicate compliance defects. The Contractor shall communicate changes to the coding standard to staff members as needed (ie.changes in Section 508 or security policies).

The Contractor shall support security, accessibility, technical standards, and architectural compliance. Security scanning is done by multiple methods and is done multiple times throughout the course of a project with methods such as penetration testing (WASA), code analysis tools (Fortify), etc. Accessibility reviews are performed through a variety of tool based and manual reviews, able to scan web applications and other technologies used for user interfaces. Architectural compliance assessments are done through submission of design materials to confirm compliance with allowed enterprise architecture. The Contractor shall expand and improve upon existing DevSecOps efforts to automate security scans, accessibility reviews, and architectural assessments.

The Contractor shall validate that the solution implementation matches the solution architecture, document any differences and submit change requests to address the differences.

The Contractor shall support prioritizing defects found during testing in the sprint backlog. Based on a prioritization, the defect could be entered in the current sprint or entered in the backlog.

The Contractor shall update the Technical Documentation Package, as required, and ensure entries made by development staff in project management tools are up-to-date so that VA stakeholders can access accurate and timely status.

In addition to the normal security testing that occurs during the SDLC, the FSC Operations team will conduct continuous security testing of FSC Productions Systems. The Contractor shall remediate defects found during continuous security testing. The Contractor shall comply with all NIST, FIPS, FISMA, OMB and VA security and privacy policy and governance as described within Section 2.0 of this PWS.

#### DEPLOYMENTS

The Contractor shall not have administrative access to any environment outside of the development environment. The Contractor shall design the architecture for the entire solution and understand how environments should be configured to support each solution. Solutions shall use a cloud architecture whenever practical to do so. In addition, the Contractor shall support Configuration Management, System Administration, and Database Administration teams to configure other environments, migrate solutions from one environment to another, and test the configurations.

The Contractor shall:

1. Create a Deployment and Installation Plan for each release. The Plan shall include all necessary instructions to create a new environment for the entire solution and describe how to move the solution from one environment to another.
2. Be the expert on the configuration of the development environment. That configuration becomes the standard for the other non-production and production environments. Assist with system roll-out to production and all other environments as requested by VA- FSC. Support developed software by assisting in deployments and by addressing technical issues.
3. Contribute to the creation of the POM (Program Operations Manual)
4. Schedule and perform knowledge transfer from development staff to team designated by the Government as the sustaining organization for the product.
5. Ensure implementation is successful; lead troubleshooting and coordinate with Configuration Management to resolve any issues related to a deployment.
6. Provide final versions of all VA-FSC Source Code and documentation for each application, systems, tools, and software developed with each change request. Documentation to be completed no later than one day prior to the planned submission to the Change Control Board (CCB)
7. Support Configuration Management, System Administration, and Database Administration with all deployment activities for the development environments.
8. Contractor shall provide recommendations for improvements upon an existing repeatable automated process for software deployment.
9. Develop an initial version of the Deployment and Installation Guide during project planning and finalize it before Critical Decision #2. The Deployment and Installation Guide will be a Configuration Item under Change Control. The Contractor shall work with the Configuration Management Team to develop/update and deliver a Deployment and Installation Guide for VA System Administrators and Database Administrators for all software development efforts. The Guide shall provide information and clear instructions on how to create an environment, configure the environment, and migrate the software build from one environment to another. The Deployment and Installation Guide shall include all environment requirements for the system including COTS, SOA components, custom-developed software, EDI, and interfaces. The Contractor shall include all necessary information to provision cloud resources. The Contractor shall develop a highly automated repeatable process to establish environments within a Cloud environment.
10. Support the rollout of enterprise level data analytics and business intelligence services. Deliver all final models used for each analytic product in the language used for the product (i.e., provide R, Python documentation)

The Contractor shall update the Technical Documentation Package to reflect deployment activities, as required prior to the deployment of each feature.

The following items are deliverables under PWS Section 5.2.3.6: Deployment and Installation Plan and Source Code. Each of these deliverables are due no later than 5 calendar days prior to submission to the Change Control Board (CCB) for approval.

Deliverables:

1. Deployment and Installation Plan
2. Source Code

#### TRANISITION TO PRODUCTION

At the direction of the government the contractor shall support migration of a product to an operations team Including knowledge transfer, contributing to the creation of product operations manual (POM), and turnover of technical documentation within 5 business days of deployment.

**Deliverables:**

1. POM

### ADDITIONAL REQUIREMENTS

In addition to performing the tasks listed in section 5.2, the staff assigned to support development in the following areas shall have the indicated knowledge and skills.

#### PEGA DEVELOPMENT

The Contractor shall provide PEGA solutions to support Customer service, Healthcare solutions and Financial services. The Contractor shall be able to support the full suite of available PEGA capabilities including but not limited to Case Management, Business Process Management (BPM), Robotic Automation, Workforce Intelligence, Autonomic Event Services (AES), and Business Intelligence Exchange (BIX). The Contractor shall establish a relationship with PEGA to ensure that FSC customers are aware of new or expanded capabilities.

When implementing PEGA solutions, the Contractors shall maximize the use of out of the box PEGA functionality and code reuse. The Contractor shall minimize the amount of custom code within each solution.

At a minimum, the contract staff assigned to support PEGA solutions will include access to staff with the following certifications: (see https://academy.pega.com/certifications)

1. Certified Pega Business Architect
2. Certified Pega System Architect
3. Certified Pega Senior System Architect
4. Certified Pega Lead System Architect
5. Certified Pega Robotics System Architect
6. Certified Pega Data Scientist
7. Certified Pega Decisioning Consultant
8. Robotic Automation badge
9. Customer Service badge

All PEGA developers will have the PEGA platform badge for the most recent PEGA release.

The contractor staff will maintain certifications and badges throughout the life of the task order.

Staff shall update certifications and badges within 6 months of a PEGA version release.

Staff will have expertise in designing Section 508 conformant user interfaces on the PEGA platform including ability to apply Section 508 controls across PEGA solutions.

#### ELECTRONIC DATA INTERCHANGE (EDI)

The Contractor shall provide expertise on developing applications that consume or process data in standard formats such as X12 and Health Level Seven Fast Healthcare Interoperability Resources (HL7 FHIR) to support the development of applications for healthcare and financial applications to support the following business activities:

1. Healthcare claim processing and payment
2. Pharmacy prescription fills
3. Healthcare eligibility verification
4. Invoice processing
5. Supply chain management including purchase orders, catalogs, and ship notices

The Contractor shall support these activities by developing the necessary EDI-related systems, applications, maps, and process procedures to ensure the timely and successful processing of electronic transactions.

The Contractor shall use designated VA-FSC development languages, editors/environments, platforms, translation and communications applications/tools, which includes, but is not limited to the following:

1. Mulesoft
2. TIBCO Foresight EDISIM and Instream
3. Compuware products - including FileAid and AbendAid
4. Gentran, Vitria BusinessWare (BW), Mulesoft, Trusted Link Enterprise (TLE), or other data translator.
5. Multiple transmission protocols - including AS2, FTP, asynchronous & synchronous connection protocols
6. VA systems such as Data Management Interface (DMI) and Mailman to receive and transmit electronic transactions
7. Cleo’s VL Trader to exchange or transfer data and/or files in a secure manner with systems or applications inside or outside the FSC
8. Java script, Oracle script, TOAD, .Net, J2EE, XML Spy, Text Pad, JBuilder, Exceed, Iron Python.

In addition, the Contractor shall provide the following sustainment activities for EDI solutions:

1. Support customer EDI activities such as conducting outreach programs and performing ASC X12 maintenance.
2. Restrict access to the data to ensure the EDI messages are authentic, properly authorized, and traceable. Protect messages from loss, modification, or unauthorized disclosure during transmission and storage.
3. Provide support services to VA FSC customers and their trading partners, as necessary, to continue successful EDI transaction transmissions.
4. Work with telecommunications and utility services providers, commercial vendors, clearinghouses, Value Added Networks (VANs) and other Government agencies to document, set up, test, and implement the necessary systems, applications, processes and procedures to exchange electronic transactions via EDI.
5. Back up VA FSC EDI developers as necessary to ensure continuity in the translation, mapping, and processing of electronic transaction or data to the appropriate file format.

### ADDITIONAL CENTER OF EXCELLENCE (COE) SUPPORT

The Contractor shall support additional COEs identified by the government. The Contractor shall provide all support for all requirements as specified in 5.1.10 Center of Excellence Support.

## TIER 3 SUSTAINMENT, PRODUCTION AND ANALYTICAL SUPPORT (T&M)

The Contractor shall provide ITIL Tier 3 software maintenance support. The Contractor shall generate tickets when software problems are identified during routine use of the tools. Using the Government-approved ticker triage process, the Contractor shall estimate the duration and anticipated level of effort to resolve the specified issue.

In addition to the execution of production support, the Contractor shall develop and maintain production support process documentation including POMs and implement process improvements to increase the FSC’s overall maturity in production support. This documentation shall be put into the Production and Analytical Support Plan. The Production Analytical Support Plan is to be delivered within 90 calendar days of task order award and updated quarterly thereafter. Any processes and tools developed by the Contractor under this TO shall be the property of the Government.

The Contractor shall:

1. Provide development and technical support to VA application administrators, developers, and production support team members.
2. Troubleshoot and resolve technical problems with the design and delivery of development services.
3. Provide emergency response services when software applications or systems disruptions occur after normal business hours to troubleshoot and potentially make changes to the source code.
4. The Contractor shall provide software maintenance necessary to improve architecture toolset performance to meet specific on-going analysis.
5. The Contractor shall provide development support for the use of architecture tool, code repositories, model or simulation used within VA FSC through a CM process. CM shall be accomplished in accordance with the process provided in VIP development methodology.
6. Participate in updating VA FSC corporate IT policies, procedures and standards related to software development and sustainment.
7. Keep abreast of required technologies, standards and methodologies and propose to the FSC how to stay current with new versions of technologies as well as legislative mandates and other items as they relate to this TO.

**Deliverables:**

1. Production and Analytical Support Plan

### SYSTEM AND APPLICATION SUSTAINMENT

The Contractor shall provide the following ITIL 3 support services for applications that fall within ATOs owned by FSC:

1. Provide sustainment support to systems and applications
2. Analyze and troubleshoot issues or problems with systems, applications, COTS software, and tools elevated by Tier 2 production support staff
3. Identify and implement systems interfaces or data transfer processes among FSC and VA systems, as well as with external (non-VA) systems
4. Identify, document, test, and implement systems, applications, and processes improvements to enable efficient and effective operations
5. Research proposed changes to existing interfaces, design modification to an existing system which will satisfy new requirements, and implement changes approved by the government
6. Set up all translation processes necessary to accept data from the trading partners and translate it to an approved output file
7. Develop and implement necessary processes and procedures to reconcile all transactions received, processed, rejected, and transmitted to/from FSC systems or applications
8. Document all incidents or issues escalated to tier 3 support and their resolutions with VA-approved tool
9. Assist in improving processes on all applicable projects to include, but not limited to, enhancements and/or streamlining of daily processes, reports, and exception handling and notification.
10. Coordinate with other FSC and VA OI&T entities on all activities that have or may have an impact on the customers’ activities and requirements and ensure the timeliness of appropriate actions.
11. Coordinate archiving issues with the appropriate VA entities based on customer requirements.
12. Monitor production processes and exception reports during the product warranty phase.
13. Transition monitoring production process and exception reports at the end of the warranty phase
14. Maintain and improve, as needed, automated processes which detect processing exceptions.
15. Diagnose and correct processing exceptions to resolve immediate problems
16. Develop and implement enhancements to prevent future failures.
17. Validate and improve, as needed, transactions processing reports. Ensure successful receipt and processing of data from different trading partners to have up-to-date reports

## OPTIONAL TASK ONE: TRAINING

This optional task shall be priced on a FFP basis. The Contractor shall provide training to Government resources and other Contract resources on SDLC methodologies, processes, and tools. This optional task can be exercised for up to 80 hours of in person training support no more than two times per period of performance throughout the duration of this TO. Training is expected to include technical topics of concern to FSC such as Agile and Pega methodologies, Pega Rules Process Commander (PRPC), and use of the Rational toolset. Other training topics include applications, tools or software delivered as part of this PWS. Additional training topics will be identified by the COR in response to evolving FSC technology support requirements. The training will be at the VA FSC site, unless otherwise authorized by the COR.

At a minimum, the Contractor shall provide a Training Plan, Training Materials and Recorded Training Sessions to support audio and visual on-demand training of past training topics. The training shall be conducted within 20 business days after the optional task is exercised. The Training Plan and Training Materials shall be delivered 5 calendar days prior to the training event and recorded training sessions shall be delivered no later than 5 calendar days after completion of the training event.

**Deliverables:**

1. Training Plan
2. Training Materials
3. Recorded Training Sessions

## OPTIONAL TASK TWO: TRANSITION SUPPORT

This optional task shall be priced on a FFP basis. It is anticipated that some work requirements will be in progress through the phase-out period of this TO. The Contractor shall provide an orderly transition of work acceptance and accomplishment, so that impact to VA FSC IT services is minimal. Interruptions or delays to the work will adversely impact the mission. Therefore, the Contractor shall provide for maximum cooperation with the successor while ensuring that no work receives inadequate attention during phase-out. The Contractor shall plan for a 30 calendar day transition period of work, to ensure continuity of services during the phase-out period.

The Contractor shall ensure a smooth transition during the next successor’s phase-in period. The Contractor shall aid the next successor in 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 successful offeror is achieved by the end of the phase-out period.

This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of all artifacts delivered under this contract, as well as existing policies and procedures, and delivery of baseline metrics and statistics. The Contractor shall develop a Transition Plan for Government approval within 10 calendar days of the optional task being exercised. The Transition Plan shall include, but is not limited to:

1. Transition of historic data to new Contractor system
2. Review, evaluation and transition of current support services
3. Coordination with Government representatives
4. Transfer of hardware and software warranties, maintenance agreements and licenses
5. Transfer of all necessary business and/or technical documentation
6. Orientation phase and program to introduce Government and Contractor personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes
7. Disposition of Contractor purchased Government owned assets
8. Update and transfer all system documentation
9. Turn-in of all Government keys, ID/access cards, and security codes
10. Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance.

**Deliverable:**

1. Transition Plan

## OPTIONAL TASK THREE: ADDITIONAL PROJECT DEVELOPMENT

The FSC is constantly evolving to meet VA priorities and may require completion of additional projects throughout the PoP of this TO. VA may exercise this optional task for additional support development of FSC projects following the software development lifecycle described in Section 5.2 of this PWS, including all subparagraphs. The specific scope of functionality to be delivered for each build in the optional task will be determined with VA Product/Project business owners prior to the start of each build cycle based on current business priorities.

It is anticipated that the mix of resources will evolve to reflect the phase of the software development lifecycle and the technical nature of the requirement. The Contractor shall provide resources to support additional project developments. This task may be exercised no more than nine times per period of performance. The period of performance of the optional task shall not extend beyond the end date of the task order period of performance in which the option is exercised.

# 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).

### 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.

### FSC DEFINED PROCESS

The Contractor shall perform their duties consistent with the processes defined by the FSC and Financial Technology Service (FTS) derived from theOIT Process Asset Library (PAL) or  The PAL scope includes the full spectrum of OIT functions and activities, such as VIP project management, operations, service delivery, communications, acquisition, and resource management. PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards and guides to assist the OIT 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 PAL includes the contractor onboarding process consistent with Section 6.2.2 and can be found at <https://www.va.gov/PROCESS/artifacts/maps/process_CONB_ext.pdf>. The main PAL can be accessed at [www.va.gov/process](http://www.va.gov/process).

### AUTHORITATIVE DATA SOURCES

The VA Enterprise Architecture Repository (VEAR) is one component within the overall EA that establishes the common framework for data taxonomy for describing the data architecture used to develop, operate, and maintain enterprise applications. The Contractor shall comply with the department’s Authoritative Data Source (ADS) requirement that VA systems, services, and processes throughout the enterprise shall access VA data solely through official VA ADSs where applicable, see below.  The Information Classes which compose each ADS are located in the VEAR, in the Data & Information domain. The Contractor shall ensure that all delivered applications and system solutions support:

1. Interfacing with VA’s Master Person Index (MPI) (formerly the Master Veteran Index (MVI)) to provision identity attributes, if the solution relies on VA user identities. MPI is the authoritative source for VA user identity data.
2. Interfacing with Capital Asset Inventory (CAI) to conduct real property record management actions, if the solution relies on real property records data. CAI is the authoritative source for VA real property record management data.
3. Interfacing with electronic Contract Management System (eCMS) for access to contract, contract line item, purchase requisition, offering vendor and vendor, and solicitation information above the micro-purchase threshold, if the solution relies on procurement data. ECMS is the authoritative source for VA procurement actions data.
4. Interfacing with HRSmart Human Resources Information System to conduct personnel action processing, on-boarding, benefits management, and compensation management, if the solution relies on personnel data. HRSmart is the authoritative source for VA personnel information data.
5. Interfacing with Vet360 to access personal contact information, if the solution relies on VA Veteran personal contact information data. Vet360 is the authoritative source for VA Veteran Personal Contact Data.
6. Interfacing with VA/Department of Defense (DoD) Identity Repository (VADIR) for determining eligibility for VA benefits under Title 38, if the solution relies on qualifying active duty military service data. VADIR is the authoritative source for Qualifying Active Duty military service in VA.

### 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 3 / High Risk** |
| --- | --- | --- | --- |
| 5.1 |  |  |  |
| 5.2 |  |  |  |
| 5.3 |  |  |  |
| 5.4 |  |  |  |
| 5.5 |  |  |  |
| 5.6 |  |  |  |

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 business 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. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
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

### 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.

#### PHYSICAL SECUIRTY REQUIREMENTS

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 FSC backup facility and surrounding property, including parking areas.

All Contractor and subcontractor personnel must 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 and/or termination of the task order for cause.

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, is not sufficient reason to warrant an extension in task order time or cost.

It is a specific condition of this task order that the Contractor, or any subcontractors performing work on this project, shall not take any photographs on or of the FSC, the FSC backup facility or satellite locations or personnel thereon, nor use or allow to be used any aspect of this TO for publicity or advertising purposes without specific written approval of the FSC’s Chief of Security Services.

Contractor and subcontractor personnel shall only park in FSC parking areas (as directed by Security Services staff) after having been issued a parking permit. Parking is provided on a “first-come, first-served” and “space available” basis. Should all designated Contractor parking spaces be in use, other contract vehicles must be parked off the Government property and the Contractor shall make other arrangements for transporting personnel to the site. 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. CST 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 COR 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 COR and Physical Security Officer.

The FSC reserves the right to exclude or remove from the site any employee of the Contractor or subcontractor whom the Physical Security Officer deems careless, insubordinate, unsafe or otherwise objectionable. Anyone with a concern regarding these characteristics of a Contractor employee may contact the Physical Security Officer for consultation. The COR shall be notified of any Contractor or subcontractor personnel removed from the site.

#### 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 access in and out of the FSC), and only during the hours it is open (Monday – Friday, 8:00 a.m. to 4:00 p.m. CST excluding official Government Holidays All items will be manually inspected (this includes opening and inspecting all packages) prior to being allowed entry.

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 always escorted 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.

#### VA REQUIRED SECURITY TRAINING

Please refer to Addendum B for training and deliverable information.

## 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** |
| A. Technical / Quality of Product or Service | Shows understanding of requirements  Efficient and effective in meeting requirements  Meets technical needs and mission requirements  Provides quality services/products | Satisfactory or higher |
| B. Project  Milestones and Schedule | Quick response capability  Products completed, reviewed, delivered in accordance with the established schedule:  Notifies customer in advance of potential problems | Satisfactory or higher |
| C. Cost & Staffing | 1. Maintains at least 95% utilization of total LOE for T&M requirements  2. Key personnel backfilled within 20 business days after receiving government approval.  3. Approved vacancies are not left unfilled for more than 30 business days.  4. Currency of expertise and staffing levels appropriate  5. Personnel possess necessary knowledge, skills and abilities to perform tasks | Satisfactory or higher |
| D. Management | 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 system access to the Government VA network to authorized contract staff as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

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

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, 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.

## GOVERNEMENT 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. 1 laptop, 2 monitors, and other associated peripherals (standard keyboard, standard mouse and a docking station) will be provided to staff requiring government furnished equipment.

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 via a monthly GFE status report. This report is initially due 30 calendar days after TO award and shall be updated no less than monthly.  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

Deliverable:

1. GFE Status Report

## RECORDS MANAGEMENT OBLIGATIONS

1. Applicability

This clause applies to all Contractors whose employees create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists.

1. Definitions

“Federal record” as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them.

The term Federal record:

1. Includes Veterans Affairs records.

2. Does not include personal materials.

3. Applies to records created, received, or maintained by Contractors pursuant to their VA contract.

4. May include deliverables and documentation associated with deliverables.

1. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

4. The VA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of VA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to the VA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government’s behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to VA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and VA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with VA policy.

8. The Contractor shall not create or maintain any records containing any non-public VA information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. The VA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which the VA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

11. Training. All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take VA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

# 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. Notice of the Federal Accessibility Law Affecting All Information and Communication Technology (ICT) Procurements (Section 508)

On January 18, 2017, the Architectural and Transportation Barriers Compliance Board (Access Board) revised and updated, in a single rulemaking, standards for electronic and information technology developed, procured, maintained, or used by Federal agencies covered by Section 508 of the Rehabilitation Act of 1973, as well as our guidelines for telecommunications equipment and customer premises equipment covered by Section 255 of the Communications Act of 1934. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

* 1. Section 508 – Information and Communication Technology (ICT) Standards

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule/text-of-the-standards-and-guidelines>. A printed copy of the standards will be supplied upon request.

Federal agencies must comply with the updated Section 508 Standards beginning on January 18, 2018. The Final Rule as published in the Federal Register is available from the Access Board: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-ict-refresh/final-rule>.

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)

E204 Functional Performance Criteria

E206 Hardware Requirements

E207 Software Requirements

E208 Support Documentation and Services Requirements

* 1. Compatibility with Assistive Technology

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

* 1. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

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

1. 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.
18. INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13834, “Efficient Federal Operations”, dated May 17, 2018; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

* 1. EPEAT

EPEAT product compliance is not required in this acquisition.

* 1. ENERGY STAR

Energy Star product compliance is not required in this acquisition.

* 1. FEMP

FEMP or FEMP low standby power product compliance is not required in this acquisition.

# 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. INFORMATION SYSTEM DESIGN AND DEVELOPMENT
16. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*
17. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 10 and future versions, as required.
18. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.
19. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
20. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information* *Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
21. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
22. The Contractor/Subcontractor agrees to:
    1. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:
       1. The Systems of Records (SOR); and
       2. The design, development, or operation work that the Contractor/Subcontractor is to perform;
    2. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
    3. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.
23. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.
    1. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
    2. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
    3. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.
24. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.
25. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.
26. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.”)*.*
27. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.
28. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE
    1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor’s security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).
    2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
    3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor’s systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection security agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.
    4. The Contractor/Subcontractor’s system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.
    5. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.
    6. VA prohibits the installation and use of personally owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.
    7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.
    8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:
29. Vendor must accept the system without the drive;
30. VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
31. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
32. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;
33. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
34. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
35. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.
36. 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.
37. 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.
38. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day’s 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

The Contractor shall comply with all mandatory and required VA FSC TMS training. The required training changes periodically but current examples include: VA Privacy and Information Security Awareness and Rules of Behavior, and Health Insurance Portability and Accountability Act (HIPAA), Contractor Rules of Behavior in accordance with Section 9, Training, from Appendix C of the VA Handbook 6500.6, “Contract Security.”

The Contractor shall submit of VA Privacy & Info Security Awareness & Rules of Behavior for all individuals engaged on the task to verify compliance. All other mandatory and required training will be verified via ‘FSC Training Compliance Report’ provided by FSC training administrators.

The Contractor may be requested to complete or provide a recommendation to the Government to complete additional training. Additional training shall be regarded as any implementation of technology or project management methodology that directly applies to the performance of this TO, that will enable faster delivery to the Government or improve overall product quality. At least 10 days prior to scheduling such any additional training, the Contractor shall submit a list of resources that will attend specified training. Training hours will be entered into ABC as applicable and will be invoiced against performance of PWS paragraphs 5.2 and/or 5.3 dependent upon the requirements the training aligns with, and benefit to the Government for approval. Once training is completed, the Contractor shall submit the training certifications for the resources approved to take the training.

1. 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:
2. 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;
3. Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS 2.0 # VA 10176) and complete this required privacy and information security training annually;
4. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.
5. 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 calendar days of the initiation of the contract action and annually thereafter, as required.
6. 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.

**Deliverables:**

1. Signed Contractor Rules of Behavior
2. Training certificates