

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS

Office of Information & Technology

Enterprise Command Operations (ECO)

Enterprise Service Desk (ESD) Tier One Support

Date**:** February 23, 2024

VA-24-00054952

**PWS Version Number:** 1.0

Contents

[1.0 BACKGROUND 4](#_Toc159835078)

[2.0 APPLICABLE DOCUMENTS 5](#_Toc159835079)

[3.0 SCOPE OF WORK 8](#_Toc159835080)

[4.0 PERFORMANCE DETAILS 9](#_Toc159835081)

[4.1 PERFORMANCE PERIOD 9](#_Toc159835082)

[4.2 PLACE OF PERFORMANCE 9](#_Toc159835083)

[4.2.1 ON-SITE ACCESS FOR GOVERNMENT PERSONNEL 10](#_Toc159835084)

[4.3 HOURS OF COVERAGE 10](#_Toc159835085)

[4.4 TRAVEL 10](#_Toc159835086)

[5.0 SPECIFIC TASKS AND DELIVERABLES 10](#_Toc159835087)

[5.1 MULTI VENDOR SERVICE PROVIDER ENVIRONMENT 11](#_Toc159835088)

[5.2 PROJECT MANAGEMENT 12](#_Toc159835089)

[5.2.1 CONTRACTOR PROJECT MANAGEMENT PLAN 12](#_Toc159835090)

[5.2.2 TECHNICAL KICK-OFF MEETING 12](#_Toc159835091)

[5.2.3 ESTABLISHMENT OF EXECUTIVE OVERSIGHT COMMITTEE 13](#_Toc159835092)

[5.2.4 ESTABLISHMENT OF A MANAGED SERVICES OVERSIGHT COUNCIL 14](#_Toc159835093)

[5.2.5 REGULAR MEETINGS AND CONFERENCE CALLS 14](#_Toc159835094)

[5.2.6 CONTRACTOR PERSONNEL 15](#_Toc159835095)

[5.2.7 REPORTING REQUIREMENTS 15](#_Toc159835096)

[5.2.8 ONBOARDING/OFFBOARDING 16](#_Toc159835097)

[5.3 TRANSITION AND TRANSFORMATION (T&T): TRANSITION-IN 16](#_Toc159835098)

[5.3.1 TRANSITION-IN PHASES 18](#_Toc159835099)

[5.3.1.1 ONBOARDING PHASE 19](#_Toc159835100)

[5.3.1.2 PRE-PLANNING PHASE 19](#_Toc159835101)

[5.3.1.3 TIER 1 SERVICE TRANSFER PHASE: 20](#_Toc159835102)

[5.4 MANAGED SERVICES REQUIREMENTS 23](#_Toc159835103)

[5.5 SUPPORT FOR VIP END USERS 28](#_Toc159835113)

[5.6 KNOWLEDGE MANAGEMENT 28](#_Toc159835114)

[5.7 OPTIONAL TASK ONE -SPANISH SPEAKING OPTION 32](#_Toc159835154)

[5.8 OPTIONAL TASK TWO – TRANSITION OUT 33](#_Toc159835160)

[5.8.1 TRANSITION-OUT TEAM AND REQUIREMENTS PLANNING 33](#_Toc159835161)

[5.8.2 TRANSITION-OUT PLAN 33](#_Toc159835162)

[6.0 GENERAL REQUIREMENTS 35](#_Toc159835163)

[6.1 ENTERPRISE AND IT FRAMEWORK 35](#_Toc159835164)

[6.1.1 35](#_Toc159835165)

[6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) 35](#_Toc159835166)

[6.1.3INTERNET PROTOCOL VERSION 6 (IPV6) 37](#_Toc159835167)

[6.1.4 TRUSTED INTERNET CONNECTION (TIC) 37](#_Toc159835168)

[6.1.5 STANDARD COMPUTER CONFIGURATION 37](#_Toc159835169)

[6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP) AND PRODUCT LINE MANAGEMENT (PLM) 38](#_Toc159835170)

[6.1.7 PROCESS ASSET LIBRARY (PAL) 38](#_Toc159835171)

[6.1.8 AUTHORITATIVE DATA SOURCES 39](#_Toc159835172)

[6.1.9 SOCIAL SECURITY NUMBER (SSN) REDUCTION 39](#_Toc159835173)

[6.2 SECURITY AND PRIVACY REQUIREMENTS 40](#_Toc159835174)

6.2.1[POSITION/TASK RISK DESIGNATION LEVEL(S) 40](#_Toc159835175)

[6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 41](#_Toc159835176)

[6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 42](#_Toc159835177)

[6.4 PERFORMANCE METRICS 43](#_Toc159835178)

[6.4.1 SERVICE LEVEL FRAMEWORK 43](#_Toc159835179)

[6.4.2 ASSESSMENT FOR MISSED SERVICE LEVELS 43](#_Toc159835180)

[6.4.3 SERVICE LEVEL REQUIREMENTS 44](#_Toc159835181)

[ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 47](#_Toc159835182)

[ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 53](#_Toc159835183)

# BACKGROUND

The Department of Veterans Affairs (VA or “Government”) is committed to creating an interactive experience for its technology users that is easy, pleasant, effective, and personalized. As part of this commitment, the VA is seeking to improve its efficiency and effectiveness of interactions by maintaining Tier-0 (Self-Service Services) and Tier-1 (Enterprise Service Desk (ESD) Services) via a Multi-Vendor Service Provider (MVSP) approach, inclusive of a Tier-1 prime vendor as well as a Contract Center Infrastructure (CCI) vendor from a separate contract.

The purpose of this PWS is to establish a Task Order (TO) that enhances service delivery, reduces cost, increases business focus, and improves the quality of Information Technology (IT) Services to End Users.

The following are key business objectives the VA expects to maintain and enhance the end user experience through vendors partnering via an MVSP environment:

* Improve VA End User efficiency and effectiveness by adopting and leveraging existing knowledge databases within VA’s IT Service Management (ITSM) tool and leading IT service management practices in the areas of customer logging, tracking, reporting, and resolving of IT Tickets and service Requests.
* Improve efficiency and effectiveness by, early identification and Problem Resolution of Root Causes of technical issues including working with specialized Resolver Groups, such as VA staff and designated third parties, before they become trends.
* Improve IT customer service and Ticket Resolution speed through continuous Service Availability (24x7x365), self-service capabilities, and skilled personnel in the areas of industry standard IT products and services.

Each Contractor shall collaborate in an environment where Incidents and Requests for all applications and related infrastructure services related to End User Tier-0 and Tier-1 Services, are received, monitored, tracked, and successfully resolved. IT service management practices used to support the delivery of Services shall be based on Information Technology Infrastructure Library (ITIL) best practices and any subsequent version of ITIL adopted in the IT industry and approved for use by VA. This ITIL based framework is a product of VA Office of Information and Technology’s (OIT) collaboration with business partners and industry and is being adopted to identify areas of improvement within the VA’s current organizational landscape.

The Tier-1 Contractor and CCI Contractor shall provide a comprehensive Managed Services solution to support VA requirements for the Services briefly described below and as further defined within Section 5.4 (Managed Services Requirements). The MVSP shall support all VA staff located in Continental United States (CONUS) or Outside of the Continental United States (OCONUS) (e.g., American Samoa, Guam, Philippines, and Germany). All Services are to be provided in the English language, with Spanish Speaking service option as outlined in Optional Task Four.

The scope of the ESD is to provide IT support to all End Users, VA designated executives/executive assistants/ VIP End Users, on a 24x7x365 basis. The contractor shall serve as the Single Point of Contact (SPOC) for all VA End Users (VA employees and VA designated third parties that use or have access to VA approved applications, hardware, software, data, and services that enable them to conduct daily business). The Contractor also shall be responsible for the end-to-end ticketing of all approved VA technologies and will work with the VA’s IT Department and appropriate third parties that provide IT support or services to ensure VA employees, and VA designated third parties are not impeded by, or prevented from, conducting daily business operations due to issues with VA applications, hardware, software, or data networks. In addition, the Contractor shall provide the ability to remotely manage, diagnose, and resolve issues related to VA desktops, laptops and notebooks, and software. Remote management services are those Services required to manage and control such devices and software over the network. This includes, maintaining and troubleshooting the operating systems and supported applications on such devices electronically to minimize the need to dispatch technical personnel, as well as fulfill approved service Requests (including access Requests).

As part of the Services, a separate Contact Center Infrastructure (CCI) vendor will provide, manage, and maintain an Automated Call Distributor (ACD) and Interactive Voice Response (IVR) system, currently the NICE CXOne platform, that integrates with the VA Information Technology Service Management (ITSM) Tool, and deliver services in accordance with ITIL service-based management processes and procedures. In addition, the vendor will develop and conduct customer satisfaction surveys (as required by management) to measure, analyze, and report results as a means to improve End User Service

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

# SCOPE OF WORK

The Contractor shall serve as one of the vendors in the MVSP environment to provide Tier-0 and Tier-1 Services. The Contractor shall handle Tier 0/Tier 1 ITSM Incident and Service Requests in accordance with standard operating procedures and Service Level Agreement thresholds. These Services will include the technical, logistical, and programmatic services to fulfill the requirements of this PWS.

The Contractor’s solution shall utilize VA’s selected ITSM tool, currently ServiceNow (SNOW), however, this may change during Period of Performance (PoP). The industry standard ITSM to be utilized will be selected by VA. Should the ITSM tool be updated, the contractor will be required to transition to the new tool. As such, the Contractor shall be required to perform a second transition to the selected ITSM Tool after Transition-In. This Service delivery Environment will be supported by an ACD and IVR system (NICE CXone) that is provided and managed by a different vendor in the MVSP environment.

The Contractor’s Services shall be able to dynamically scale in real-time to VA’s volumes, including temporary surges of demand, with no degradation of committed Service Levels. The VA ESD covers approximately the following:

• Customer Base: ~500K VA internal employees/contractors

• Supports: ~ 900 Applications

• Call Volume: ~250K calls offered per month

• Chat Volume: ~2000 chats offered per month

• Tier 1 Incidents and Requests created ~ 3,000,000 annually

• Provides 365 Days 24/7 operation that is a centralized desk supports all VA internal employees/contractors including VIPs ~ 1700 senior executives and their executive assistants, that can respond to a host of issues involving hardware, and affected, software, applications, system access, password reset, facility and security.

The performance/functions outlined throughout the PWS are considered non-inherently governmental functions IAW Federal Acquisition Regulation (FAR) Subpart 7.7, and non-personal services IAW FAR 37.104.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The Period of Performance (PoP) shall be a 12-month base period, with four (4) twelve-month option period- and two optional tasks, to be exercised at the Government’s discretion.

The base period shall include tasks described in PWS sections 5.0 through 5.5. All Option Periods shall include tasks described in PWS sections 5.0, 5.1, 5.2, 5.4, and 5.5.

Included are Optional tasks Spanish Speaking Option (5.7) and Transition-out Services (5.8).

The total PoP shall not exceed 60 months.

## PLACE OF PERFORMANCE

Efforts under this contract shall be performed at Contractor facilities that shall be located within the continental United States. The Contractor shall identify the Contractor’s place(s) of performance in the Contractor Project Management Plan (CPMP). Remote telework by contractor personnel must be pre-approved by the COR. Remote telework for agents providing Tier 1 services must be distraction free to prevent degradation of services. Any degradation in services shall be grounds to revoke telework capabilities at the sole discretion of VA through modification of the contract.

### ON-SITE ACCESS FOR GOVERNMENT PERSONNEL

The Contractor shall provide a workspace at the Contractor facilities for two (2) VA employees. This workspace will provide VA employees with the ability to view real time managed Services performance data, and the rights to pull service agent activity and Call traffic related reports while at the Contractor facilities. The Contractor shall provide or make available reasonable office equipment and supplies for VA personnel to assist in the administration of the Services, including the following:

* Workspace
* Telephone
* Access to a printer
* Local Area Network (LAN) access (either wired or wireless)

## HOURS OF COVERAGE

Services shall be provided to End Users 24 hours a day, 7 days a week, 365 days a year (24x7x365).

## TRAVEL

During the base period, and any of the option periods, if exercised, VA anticipates requiring two (2) people for four (4) trips per year to either Washington, DC or Austin, TX for executive level meetings. The duration of each trip will be four (4) calendar days. These costs will not be directly reimbursed by the VA.

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall provide the Services identified in this Section in the manner described in this PWS.

The Contractor shall provide all technical and management services to support the task, including program management, technology management, information and relationship management, human resources management, performance management, quality assurance/quality improvement, management reports, security, contingency/disaster recovery, and value engineering, as described in this PWS. All deliverables/work products shall be considered the intellectual property of VA. Intellectual property shall not be used outside of this contract without the express written consent of the Contracting Officer (CO) in coordination with the VA PM.

The Contractor shall furnish the necessary facilities, personnel, equipment, supplies, and services, as required, to meet the requirements of VA as established herein with the capability to support a wide range of communication channels (e.g., telephone, text, WebChat). In addition, the Contractor shall use existing enterprise toll-free numbers unless otherwise directed. The Contractor shall provide Services and perform all technical and management functions, as described in this PWS, to plan, design, implement, operate Tier-1 solutions. The Contractor shall also manage Tier-0 or self-service support (e.g., triaging tickets submitted through the self-service portal).

The Contractor must be prepared to, and will be required to, perform all Services relative to any and all actual contact volumes during the aforementioned PoP, notwithstanding the estimated volumes identified herein.

## MULTI VENDOR SERVICE PROVIDER ENVIRONMENT

ESD services will be provided in a MVSP environment. Disparate contractors will provide complementary services, including the contact center infrastructure and Tier 1 agent services. The Government requires a prime contractor providing the CCI services and a prime contractor providing the Tier 1 agent services, simultaneously. The Government expects these contractors to work cooperatively to the maximum extent possible to ensure seamless, high quality customer service.

The Contractor shall attend all VA-required (virtual and/or onsite) meetings in conjunction with other MVSPs to coordinate with other contractors and entities as described herein.

Any and all materials and communications used to accomplish the work under this Contract shall be non-proprietary and be able to be used collaboratively by MVSP.

As such the Contractor shall ensure activities in support of this Contract are effectively coordinated with ESD stakeholders and other contractors. Where multiple contractors (under separate contracting vehicles) are involved in a task, the Contractor shall not communicate with other contractors without prior notification and approval from the CO, COR, and VA PM.

Activities and areas requiring Contractor coordination and cooperation shall include, but are not limited to, the following:

1. Comprehensive cross-area support and consistent messaging. This includes areas where functional area processes overlap with other program area processes, common data re-use requirements, and data and report submission standards. This interaction and coordination will be ongoing and applies broadly to all aspects of this Contract (e.g., common call flows and scripts, QA monitoring and reporting).
2. The functions/capabilities handoffs between the Contractor, ESD stakeholders, and other MVSP contractors, ensuring coordination and collaboration to provide holistic strategies, solutions, and reporting. For example:
   1. Participation in call-flow testing as well as test calls before go-live events to assess performance and capture any lessons learned
   2. Developing or revising procedures, scripts and use cases to ensure successful execution of services and transfer of tickets and tasks
   3. Knowledge management and sharing
3. Adhere to VA approved communications, governance, and quality assurance processes.
4. Share all deliverables, systems, data, and tools created from this Contract with stakeholders, at the request of the COR.
5. Contractors shall work cooperatively to identify service improvements and other efficiency projects relevant to CCI and Tier 1 processes and, if any are identified, the Contractor shall assign sufficient staff support to seek to develop process solutions that could be implemented.
6. Collaborate and maintain a balance of interests, transparency, open, honest, frequent, and comprehensive communication to build and maintain relationships of trust and respect.
7. Contractor shall fully cooperate with ESD and its contractors during timeframes when other contractors are in transition phases such as transition in and out.

## PROJECT MANAGEMENT

### 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 contract 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 contract. The Contractor shall update and maintain the VA Program Manager (PM) approved CPMP throughout the PoP. The Plan shall include a subsection on how the Contractor intends to encourage and facilitate the hiring of Veterans in accordance with the PWS.

**Deliverable**:

1. Contractor Project Management Plan

### TECHNICAL KICK-OFF MEETING

A technical kickoff meeting shall be held within 10 business days after award. The Contractor shall coordinate the date, time, and location (can be virtual) with the CO, as the Post-Award Conference Chairperson, the VA PM, as the Co-Chairperson, the Contract Specialist (CS), and the COR. The Contractor shall provide a draft agenda to the CO and VA PM at least five (5) business 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 ESD Tier 1 Support. The Contractor shall submit the final updated presentation to the CO for review and signature within three (3) business days after the meeting. The Contractor shall also work with the CS, the Government’s designated note taker, to prepare and distribute the meeting minutes of the kickoff meeting to the CO, COR, and all attendees within three (3) business days after the meeting. The Contractor shall obtain concurrence from the CS on the content of the meeting minutes prior to distribution of the document.

### ESTABLISHMENT OF EXECUTIVE OVERSIGHT COMMITTEE

The Contractor shall designate representative members with the appropriate skills and experience to serve on the Executive Oversight Committee (EOC) which will be chaired by VA and comprised of a number of key executives from the Contractor and VA, which will meet, at a minimum, on a quarterly basis, and at such time as its members deem appropriate, to perform the following activities:

* Review and analyze the monthly performance reports for the preceding period, including any schedule overruns, Service Level attainment of targets, and any issues or Service Outages that affect Contractors’ overall performance
* Review and discuss progress on the Resolution of issues
* Attempt to Resolve, or designate individuals to attempt to Resolve, escalated Issues
* Review and attempt to address escalated decisions
* Prepare and deliver a Quarterly Review presentation. Presentation shall be delivered no later than two business days prior to the scheduled EOC meeting.

Contractor members of the Executive Oversight Team will include the Contractor Account Executive Sponsor, and Contractor Account Executive(s) providing oversight to this contract. The Contractor shall provide to VA for review and approval an EOC charter identifying the members, roles/responsibilities, and processes for the EOC.

**Deliverable:**

1. EOC Charter
2. Quarterly Review presentation

### ESTABLISHMENT OF A MANAGED SERVICES OVERSIGHT COUNCIL

The Contractor shall designate representative members with the appropriate skills and experience to the Managed Services Oversight Council (MSOC) which will be chaired by the VA Supplier Management Executive and will meet monthly to address business requirements, contract performance, performance standards, continuous improvement, benchmarking, quality assurance and escalated issues and disputes. The Contractor shall identify a Single Point of Contact (SPOC) who will provide oversight to this contract and will serve as the Contractor’s highest-ranking representative on such council and have the authority to commit the Contractor (subject to VA reviews and approvals) to implement the course of action as deemed necessary by VA.

Prepare and deliver a Monthly Review presentation. Presentation shall be delivered no later than two business days prior to the scheduled MSOC meeting.

**Deliverable:**

1. Monthly Review presentation

### REGULAR MEETINGS AND CONFERENCE CALLS

Contractor and VA representatives shall meet periodically to discuss matters arising under this PWS. Such meetings shall include the following:

* The meetings by the committee and council noted above
* Such other meetings of VA and the Contractor personnel, including senior management of the Contractor, as the Government may reasonably request

For each such meeting, the Contractor shall prepare an agenda which will incorporate the topics designated by VA. The Contractor shall distribute the agenda within five (5) business days of each meeting so that the meeting participants can prepare. In addition, the Contractor shall record, and distribute minutes for every meeting for review and concurrence by the Contracting Officer’s Representative (COR) within three (3) business days.

The Contractor shall notify the COR in advance of scheduled meetings with VA representatives or designated alternates (other than meetings pertaining to the provision of specific Services on a day-to-day basis) and shall invite the COR (or whomever the COR designates) to attend such meetings.

**Deliverable:**

1. Regular Meeting Agenda
2. Regular Meeting Minutes

### CONTRACTOR PERSONNEL

The Contractor shall ensure that all supervisory and/or management personnel and support staff (not to include agents) are ITIL Foundations certified to the latest ITIL version. The Contractor shall also ensure that all Incident Managers have specific incident management experience (preferably 3 years or more) in the VA environment. The contractor shall ensure all personnel with active VA network access accounts remain active.

### REPORTING REQUIREMENTS

The Contractor shall provide the COR with weekly progress reports in electronic format. VA preference for these reports is Microsoft (MS) Word and MS Project formats.  These reports shall reflect data as of the last day of the preceding week***.*** The weeklyprogress reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period.  The weekly progress report shall include detailed instructions and explanations for each required data element to ensure that data is accurate and consistent. The report shall identify any issues that arose and a description of how the issues were resolved.  If issues have not been completely resolved, the report shall include a discussion of the issue, actions taken to resolve, and an explanation of the Contractor’s plan and timeframe for resolving the issue. The report shall also include an itemized list of all Information and Communication Technology (ICT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. The Contractor shall keep in communication with VA as needed to ensure that issues that arise are transparent to both parties.

The table below describes the Service reports in addition to the weekly progress report to be provided by Contractor to the VA in accordance with this PWS. It includes a summary description of the content and frequency of such Service reports.

| **Service Report Deliverables** | **Description** | **Frequency** |
| --- | --- | --- |
| Service Management Report | * Summary of accomplishments, work in progress, and planned work. * Review of resource allocation for past year and progress as compared to road map (goals and objectives). * Attrition rate for the previous month | Monthly |
| Service Portfolio Management Report | * Review of latest Systems and Applications * List of solutions and capabilities needed to meet emerging requirements for ESD support | Quarterly |
| Contractor Personnel Certifications | * Status of ITIL Foundation Certification of all required Contractor Personnel. List of certification level, currency (valid / expired) and renewal status. | Quarterly |

**Deliverables**:

1. Weekly Progress Report
2. Security and Virus Incidents Report
3. Service Management Report
4. Service Portfolio Management Report
5. Contractor Personnel Certifications

### ONBOARDING/OFFBOARDING

The Contractor shall manage the onboarding and offboarding of its staff. Onboarding includes steps to obtain a VA Personal Identification Verification (PIV) card, network and email account, complete VA required training, initiate background investigations, and gain physical and logical access. In addition, the Contractor shall identify individuals who may require elevated privileges to the necessary development and test environments for the various Systems.

A Contractor Onboarding SPOC shall be designated by the Contractor that tracks the onboarding and offboarding status of all Contractor personnel. The Contractor Onboarding SPOC shall be responsible for complete, accurate and timely submission of all required VA onboarding and offboarding paperwork to the VA COR. The Contractor shall be responsible for tracking the status of all its staff’s onboarding activities to include the names of all personnel engaged on the task, their initial training date for VA Privacy and Information Security training, their next required training date and PIV status. The Contractor Onboarding SPOC shall also report the status at the staff level during status meetings. The Contractor shall provide an Onboarding/Offboarding Status Report weekly for any staff with outstanding onboarding requests for review by the COR. The Contractor shall provide a bi-monthly all staff roster.

**Deliverable**:

1. Weekly Onboarding/Offboarding Status Report
2. All Staff Roster

## TRANSITION AND TRANSFORMATION (T&T): TRANSITION-IN

The Contractor shall have one hundred and fifty (150) calendar days from contract award to service 100% of the Enterprise Service Desk (ESD) workload at a performance level that meets the Service Level Agreements (SLAs). The Contractor shall identify a Project Manager to plan, execute and monitor Transition-in activities and work with the Government and the outgoing Contractor to ensure a smooth, timely and complete transfer of services.

To maintain continuity of services and minimize potential negative effects during transitional phases, the Contractor shall develop a comprehensive Transition-In plan that describes the activities and processes needed to complete the Transition-in phases within the 180-day timeframe, which includes a 30-day stabilization period.

The Contractor shall:

1. Provide phase-in transition planning and execution of all PWS-specific tasks during the transition period handing off work from outgoing Contractor to the incoming Contractor.
2. Work closely with the outgoing contractor, VA, and other stakeholders to ensure knowledge transfer is thorough and all encompassing, to include: The transfer of all applicable hardware, software, licenses, services, information stores, configuration and asset repositories, operational and development processes, documentation, knowledge stores, and any other resource associated with the services. The transition planning shall include capturing knowledge of the current ESD design, implementation, and operations.
3. Conduct an initial Transition-in Planning meeting within five (5) business days after the contract kickoff meeting, with the VA COR, VA organizations identified by the COR, the ESD PMO, and outgoing Contractor resources
4. Document the approach and milestones to transfer the full support requirements responsibilities in a Transition-in Plan.

The Transition-in Plan shall include at a minimum:

1. Review of program documentation
2. The plan to participate, as an observer of services and metrics performed by the incumbent Contractor for the purpose of facilitating knowledge transfer
3. Milestone schedule of transition activities
4. Roles and Responsibilities matrix showing key personnel
5. The plan to transition current support services
6. Details on accessing and assessment of systems and tools
7. Transition coordination schedule to meet with Government and Contractor representatives, including all VA organizations that hold responsibilities, to confirm demarcation of responsibilities and interface points for performance of work elements
8. Transition schedule with tasks, duration, milestones, resource allocation, knowledge transfer sessions, and dates for completion of work transfer to Contractor
9. Risks and associated risk mitigation plans
10. Summary and schedule for Government-required training, clearance, and certifications.

The base year of the contract will include overlap opportunities between the incoming and outgoing ESD Contractors where both Contractors share responsibility for providing services during a contract transition period, and where the outgoing Contractor provides necessary training and assistance to the new Contractor to ensure continuity of services. Updates to the Transition-in plan can occur as needed and must be approved by the Government. Approved changes to the Transition-in plan shall be captured in a revised version of the plan, which shall be disseminated to all stakeholders.

The Contractor shall develop an On-Boarding Plan to ensure onboarding actions are performed in an accurate and timely manner throughout the period of performance, especially actions related to access to VA computer systems, and other security requirements. Additionally, the Contractor shall develop a Contractor Resource Continuity Plan that supports Contractor resource continuity, focused on retaining quality contract resources and provisions for timely resource backfill during unprogrammed turnover and/or a surge in service requirements.

**Deliverables:**

1. Transition-In Plan
2. On-Boarding Plan
3. Contractor Resource Continuity Plan

### TRANSITION-IN PHASES

The Transition-in is comprised of the following phases, as described more fully below:

1. **Onboarding** – onboarding of Contractor personnel following contract award.
2. **Pre-Planning** – All activity associated with preparation in advance of engaging VA’s subject matter expert (SME) community and the out-going contractor for knowledge acquisition.
3. **Tier 1 Services Transfer** – All activity associated with the transfer of Tier 1 services from the outgoing Contractor to the incoming Contractor. This phase shall be conducted in four stages, each of which will result in the Contractor assuming responsibility of a fixed percentage of customer contacts until 100% of all contacts are assumed at the end of this phase. For Stage 1 the contractor shall assume 25% of customer contacts, for Stage 2 the contractor shall assume 50% of customer contacts, for Stage 3 the Contractor shall assume 75% of customer contacts, and for Stage 4 the Contractor shall assume 100% of customer contacts.

The Government will utilize the following gates to evaluate the Contractor’s readiness to proceed to the next stage/phase. Evaluation of the Contractor’s readiness will be based on the incoming Contractor’s performance in meeting its SLA metrics.

If the Contractor is deemed “not ready” to enter the next phase by the Government, then the Contractor shall issue a credit. The credit is calculated as 12.5 percent of the Monthly Recurring Charge (MRC) for that service. Further, if the Contractor fails to meet the SLA performance objective for two consecutive months, the Contractor must credit the Agency 25 percent of the MRC for that service; failure to meet the SLA performance objective for three consecutive months requires a credit of 50 percent of the MRC for that service. After the third consecutive month of failure to perform at the specified level, the Agency may discontinue the service through termination of contract.

1. Quality Gate #1 – Exit Detailed Pre-Planning Phase - Entry into Tier 1 Services Transfer Phase
2. Quality Gate #2 – Exit Tier 1 Services Transfer Phase Stage 1 - Entry of Stage 2
3. Quality Gate #3 – Exit Tier 1 Services Transfer Phase Stage 2 - Entry of Stage 3
4. Quality Gate #4 – Exit Tier 1 Services Transfer Phase Stage 3 – Entry of Stage 4
5. Quality Gate #5 – Exit Tier 1 Services Transfer Phase Stage 4

The following is a detailed description of the phases and the requirements of each:

#### ONBOARDING PHASE

* 1. Overall Approach

The Onboarding phase consists of the activities associated with bringing Contractor personnel into the VA environment in a manner consistent with the contract. This is a continuous process throughout the PoP of the contract and may run concurrently with the other phases described herein.

* 1. Contractor Onboarding Requirements
     + 1. Provide qualified staffing resources to deliver Tier 1 services in a manner that meets SLAs as defined in this PWS
       2. Escalate any on-boarding issues immediately to the PM, COR, and CO
       3. Report on-boarding/off-boarding status/metrics in the weekly status report

#### PRE-PLANNING PHASE

* 1. Overall Approach

Pre-planning is a period in which Contractor develops the overall transition approach for the Services, prepares the Contractor personnel through education and training before the Tier 1 Services Transfer phase.

* 1. The Pre-planning phase shall include, but may not be limited to, the following activities:

1. Ensure proper access to required resources, systems, including telephony, and application is granted for all onboarded agents
2. Ensure all required VA training is completed by all onboarded agents
3. Develop familiarity and knowledge of the Services and the VA environment including review of Documentation, run books, Problem logs, training materials
4. Update, as necessary, the Transition-in Plan for VA approval
5. Deliver Quality Gate #1 presentation demonstrating that all of these activities have been executed to secure VA agreement that the Contractor is prepared to exit the Pre-Planning phase and enter the Tier 1 Services Transfer Phase

* 1. Pre-Planning Exit Criteria
  2. VA approval of Contractor Transition In plan, On-Boarding Plan and Contractor Resource Continuity Plan.
  3. Validation that proposed training and education has been executed for Contractor resources.
  4. Validation that all Contractor staff have access to all required systems, including telephony, applications, and resources necessary to perform their required tasks.

**Deliverable:**

* + - * 1. Quality Gate #1 presentation

#### TIER 1 SERVICE TRANSFER PHASE:

1. Overall Approach

This is the period during which knowledge will be acquired and the Contractor will assume Services responsibility by performing the following activities:

1. Define knowledge areas (e.g., procedural, systems, conceptual)
2. Work with the outgoing contractor to transfer knowledge as required
3. Work with VA SMEs to transfer knowledge as required
4. Identify and remediate any gaps in knowledge transfer
5. Execute knowledge transfer techniques:
6. This includes SME interviews, process mapping, scenario-based training, review of run books, and utilization of Contractor automated tools
7. Assume the Tier 1 services from the out-going contractor in accordance with the stages outlined in the subsequent section.
8. The Contractor will assume Services responsibility using an incremental approach consisting of the following four (4) stages, which represent milestones within the Phase:

**Stage 1:**

Within sixty (60) calendar days after contract award, the Contractor shall assume responsibility for at least 25% of the total Tier 1 support workload from the out-going Contractor. This shall include all calls, live chats, and tickets in queue. The Contractor shall meet all SLA metrics.

The Contractor shall deliver the Quality Gate #2 presentation that shall include, at a minimum, the number of Contract staff onboarded to date, i.e., the number of Contract staff that have obtained access to the required VA resources; the Contract staff that have completed the training required to work independently as a Tier 1 agent, and demonstrates that their performance meets the applicable SLA metrics to obtain VA agreement that the Contractor is prepared to exit Stage 1 and enter Stage 2.

**Stage 1 Exit Criteria:**

1. The Contractor is performing at least 25% of the workload and their performance meets the Tier 1 Support SLAs requirements. The Contractor is continuing to successfully on-board and train requisite personnel to enter Stage 2.
2. All reporting and documentation performed and logged appropriately in Ticket System and document repository.
3. Active participation in VA operational meetings.

**Deliverable:**

A. Quality Gate # 2 Presentation

**Stage 2:**

Within ninety (90) calendar days after contract award, the Contractor shall assume responsibility for at least 50% of the total Tier 1 support workload from the out-going Contractor. This shall include all calls, live chats, and tickets in queue. The Contractor shall meet all SLA metrics.

The Contractor shall deliver the Quality Gate #3 presentation that shall include, at a minimum, the number of Contract staff onboarded to date, i.e., the number of Contract staff that have obtained access to the required VA resources; the Contract staff that have completed the training required to work independently as a Tier 1 agent, and demonstrates that their performance meets the applicable SLA metrics to obtain VA agreement that the Contractor is prepared to exit Stage 2 and enter Stage 3.

**Stage 2 Exit Criteria:**

1. The Contractor is performing at least 50% of the workload and their performance meets the Tier 1 Support SLAs requirements. The Contractor is continuing to successfully on-board and train requisite personnel to enter Stage 3.
2. All reporting and documentation performed and logged appropriately in Ticket System and document repository.
3. Active participation in VA operational meetings.

**Deliverable:**

B. Quality Gate # 3 presentation

**Stage 3:**

Within one hundred twenty (120) calendar days after contract award, the Contractor shall assume responsibility for 75% of the total Tier 1 support from the out-going Contractor. This shall include all calls, live chats, and tickets in queue. The Contractor shall meet all SLA metrics.

The Contractor shall deliver the Quality Gate #4 presentation that shall include, at a minimum, the number of Contract staff onboarded to date, i.e., the number of Contract staff that have obtained access to the required VA resources; the Contract staff that have completed the training required to work independently as a Tier 1 agent, and demonstrates that their performance meets the applicable SLA metrics to obtain VA agreement that the Contractor is prepared to exit the Tier 1 Service Transfer phase.

**Stage 3 Exit Criteria:**

1. The Contractor is performing 75% of the workload and their performance meets the Tier 1 Support SLAs requirements. The Contractor is continuing to successfully on-board and train requisite personnel to enter Stage 4.
2. All reporting and documentation performed and logged appropriately in Ticket System and document repository.
3. Active participation in VA operational meetings.

**Deliverable:**

C. Quality Gate # 4 presentation

**Stage 4:**

Within one hundred fifty (150) calendar days after contract award, the Contractor shall assume responsibility for 100% of the total Tier 1 support from the out-going Contractor. This shall include all calls, live chats, and tickets in queue. The Contractor shall meet all SLA metrics.

The Contractor shall deliver Standard Operating Procedures (SOPs) providing detailed descriptions of the contractor’s operational support processes. These SOPs shall be updated and delivered as required throughout the period of performance.

The Contractor shall deliver the Quality Gate #5 presentation that shall include, at a minimum, the number of Contract staff onboarded to date, i.e., the number of Contract staff that have obtained access to the required VA resources; the Contract staff that have completed the training required to work independently as a Tier 1 agent, and demonstrates that their performance meets the applicable SLA metrics to obtain VA agreement that the Contractor is prepared to exit the Tier 1 Service Transfer phase.

**Stage 4/Phase 3 (Tier 1 Service Transfer) Exit Criteria:**

1. The Contractor has successfully on-boarded and trained requisite personnel to adequately perform 100% of Tier 1 support services in a manner that meets SLA requirements.
2. All reporting and documentation performed and logged appropriately in Ticket System and document repository.
3. Active participation in VA operational meetings.

**Deliverable:**

D. Standard Operating Procedures (SOPs)

E. Quality Gate # 5 presentation

## MANAGED SERVICES REQUIREMENTS

The tables below contain detailed descriptions requirements relating to the Services.

| **Ref. #** | **Principal Activity** |
| --- | --- |
|  | **Enterprise Service Desk (ESD) Services** |
|  | **Service Strategy** |
|  | **Strategy Generation** |
|  | Provide input to OIT on related technology refreshes, upgrades, and strategies. |
|  | Provide necessary reports required for planning and analysis activities (e.g., utilization and capacity trend reports) |
|  | **Financial Management** |
|  | Provide necessary information to support VA contractual and financial accounting requirements. |
|  | **Service Portfolio Management** |
|  | Document and process all customer interactions utilizing VA provided ITSM suite. |
|  | Provide regular and recurring recommendations regarding potential improvements to the ITSM suite and supporting ITIL processes. |
|  | Support the test planning and coordination, drafting test cases, and use case testing necessary to support ITSM suite updates and upgrades*.* |
|  | Perform periodic service desk Tier 0/1 systems and tools innovation review to advise VA of emerging technologies suitable for implementation. |
|  | Provide a Service Delivery Manager contact list prioritized to ensure accountability for service delivery. Updated list shall be provided in the Quarterly Review presentation. |
|  | Provide recommendations for service improvements across the VA environment to support Tier 0/1 related activities. |
|  | Comply with all VA corporate policies, procedures, and standards. |
|  | Utilize only VA approved tools for customer interactions/triage. |
|  | **Demand Management** |
|  | Ensure acceptable levels of performance leveraging the most current workforce management tools provided by the CCI to account for changes in demand. |
|  | **Service Design** |
|  | **IT Service Catalog Management** |
|  | Provide recommendations for improvements to IT service catalog functionality and content for Tier 0/1 support. |
|  | **IT Service Continuity Management** |
|  | Provide Continuity of Operations Plans (COOP) for all Contractor Systems and tools necessary to perform Tier 0/1 services that support and integrate with the VA COOP.  Perform Disaster Recovery Exercises, both tabletop and full scale, COOPs for all contractor systems and tools necessary to perform Tier 0/1 services.  Provide Continuity of Operations for all Contractor Systems and tools necessary to perform Tier 0/1 services in the event of contingency operations. |
|  | Provide a COOP that meets VA Recovery Point and Time Objectives. |
|  | Update COOP annually following test or events, or as necessary. Provide a COOP Test Report as required. |
|  | Maintain crisis communication call and distribution lists inclusive of contract management staff, service providers and VA technical teams to ensure expedited contingency operations. |
|  | Forecast and posture for natural disasters and emergency events that may cause a disruption in Tier 0/1 Contractor Services. |
|  | Inform VA immediately about natural disasters and emergency events affecting contractor facilities and staff in accordance with established procedures. |
|  | Implement changes to COOP based on VA approved recommendations. |
|  | **Compliance Management** |
| 1.2.3.1 | Support compliance audit requests and take corrective actions as requested by VA. |
|  | **Information Security Management** |
|  | Document and maintain processes and procedures in accordance with VA security guidelines. |
|  | Provide updated Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) annually or as necessary. |
|  | **Training and Education** |
|  | Ensure VA required certifications are maintained by Contractor personnel at no expense to VA. |
|  | Ensure mission-ready staffing for all Tier 0/1 services. |
|  | Ensure all contract personnel are trained on all current/new technologies and applications relevant to Tier 0/1 services. |
|  | **Service Operations** |
|  | **Tier-1 (Enterprise Service Desk) Services** |
|  | Provide Tier 1 services via multiple electronic channels to include but not limited to:   * Telephony; * SMS/text messaging; * Chat functionality; * Service Portal. |
|  | Execute Tier 1 services in accordance with ITIL practices as adopted by VA. |
|  | **Incident Management** |
|  | Handle Tier 0 ITSM Incident tickets routed to Tier 1 queues in accordance with standard operating procedures and Service Level Agreement thresholds. |
|  | Handle/triage incidents in accordance with standard operating procedures and Service Level Agreement thresholds. |
|  | Acts as Single Point of Contact (SPOC) for user-initiated status inquiries about all tickets. |
|  | Handle/escalate urgent, business critical and VIP Incidents in accordance with established VA operating procedures. |
|  | Document actions and/or customer interactions related to Incidents in ITSM Tool. |
|  | Establish and maintain a dedicated, internal Incident Management Team (24/7/365) to participate in VA Major Incident Management process. |
|  | Identify and validate potential Major Incidents, escalate validated major incidents to the VA Major Incident Management Team, and communicate to all Tier 1 Service Providers. |
|  | **Request Fulfillment (Service Requests)** |
|  | Handle Tier 0 ITSM Request tickets routed to Tier 1 queues in accordance with standard operating procedures and Service Level Agreement thresholds. |
|  | Handle/triage requests in accordance with standard operating procedures and Service Level Agreement thresholds. |
|  | Acts as Single Point of Contact (SPOC) for user-initiated status inquiries about all requests. |
|  | Handle/escalate urgent, business critical and VIP Requests in accordance with established VA operating procedures. |
|  | Document actions and/or customer interactions related to Requests in ITSM Tool. |
|  | **Service Operation Functions** |
|  | Collaborate with other IT entities to contribute Tier 1 perspective in Problem Management process. |
|  | **Continual Service Improvement** |
|  | Recommend improvement options, based on operational analytics and observations to be provided on a regular basis (i.e., weekly, bi-weekly, or monthly timeframes). |
|  | Set and achieve annual goals for Tier 1 continuous service improvements via technology, process, or other miscellaneous changes. |
|  | Utilize agent scoreboard for operational improvements. |
|  | Leverage speech analytics for operational improvements. |
|  | Perform call monitoring for internal Contractor training purposes only. |
|  | Meet with Tier-2 and Tier-3 support teams to identify opportunities to improve the ESD’s Tier-0 and Tier-1 capabilities. |
|  | Make VA-requested changes to operations and Service delivery based upon VA quality assurance programs. |
|  | Utilize VA customer satisfaction surveys to improve operations. The contractor shall utilize responses to identify areas for improvement and provide an action plan to facilitate continuous service improvement. This action plan shall be provided in the Monthly Review presentation. |
|  | Provide communication on contractor personnel coverage strategy to include all vacations, paid time off, and surge coverage. |
|  | Establish and maintain an Operational Inquiry process which responds to all customer feedback with detailed analysis of such feedback and subsequent publication of the analysis to leadership and the customer with a 24 hour turn on the analysis as a goal. |
|  | **Process Integration** |
|  | Contractor shall attend and participate in all ESD Process Integration (PI) intake/project meetings to identify and document required Tier 1 support. |
|  | Contractor shall develop and document process flows for each call driver required for ESD Tier 1 support. |
|  | Contractor shall create all process flows required to support Process Integration using Microsoft VISIO or VA and ESD approved process flow diagram software. |
|  | Contractor shall have 7 days to complete process flows once all stakeholders agree that all call drivers have been defined and solutioned. |
|  | Contractor shall submit PDF version of process flow to all stakeholders for approval prior to submitting for creation of knowledge articles. |
|  | Contractor shall ensure finalized copy of process flow is stored in a central repository owned and managed by the VA. |
|  | Contractor shall have minimum 3 years of experience in process mapping and process flow design. |
|  | Contractor personnel shall be capable of supporting ten intake/projects per person concurrently. |

## 5.5 SUPPORT FOR VIP END USERS

The Contractor shall provide ESD (Tier-0 and Tier-1) Services for Very Important Person (VIP) End Users as identified by VA. VIP End Users will receive a higher level of Service as reflected in the Service Levels in Section 6.1.3. VIPs shall have a dedicated phone number which will connect them directly with an agent. The agents will be trained to provide VIP support, which shall be documented in the updated Training Plan. Any call from the Top 8 customer list that requires a ticket to be escalated to other Resolver Groups will be accompanied by an instant message communication (currently MS Teams). The immediate handoff of the ticket will be documented in the ITSM tool (currently ServiceNow).

## 5.6 KNOWLEDGE MANAGEMENT

The table below contain detailed descriptions requirements relating to the Services.

|  |  |
| --- | --- |
|  | **Knowledge Management** |
|  | The Contractor shall create, write, update, retire, and maintain documents (“Knowledge Articles”) in the Tier 0 (self-service) and Tier 1 repositories, which are housed in an ITIL-based tool. The Contractor shall write and maintain Knowledge Articles in plain, easy-to-comprehend language, composed for an eighth-grade intellectual capacity. |
|  | The Contractor shall develop, produce, and attach self-service instructional self-service videos with audio visual, and closed caption components that correspond to Knowledge Articles. One thousand (1,000) self-service videos shall be created annually or until all Tier 0 (Self-Service) Knowledge Articles have a coinciding cinematic. Closed caption shall be offered as an option. |
|  | The Contractor shall provide detailed documentation about their processes for creating new Tier 0 (self-service) and Tier 1 Knowledge Articles. The Contractor shall update and maintain these processes for the length of the contract. |
|  | The Contractor shall follow the “No Knowledge Article Found” process to create a new knowledge article, when no article exists in the Tier 0 (self-service) and Tier 1 repositories. |
|  | The Contractor shall provide recommendations for expanding the Tier 0 (self-service) and Tier 1 portal capabilities to the VA Knowledge Management Team for consideration of new and ever-changing technological advances. This shall be completed every three months. |
|  | The Contractor shall complete the ESD Business Case Justification form or any specified VA justification form, when providing written recommendations. |
|  | The Contractor shall create, update, and maintain clear, current, thorough, and accurate written documentation about all IT service-related standards and procedures in an approved online repository, such as SharePoint, to which VA Knowledge Management has full access. |
|  | The Contractor shall update technical, operational, Tier 0 (self-service), and Tier 1 documentation based upon analysis of Service Tickets, Submissions, Industry Changes, and Problem Management statistical trends. This documentation shall be shared with the VA Knowledge Management Team quarterly throughout the Fiscal Year. |
|  | The Contractor shall perform all steps of the “Bi-Annual Review Process” on Tier 1 and Tier 0 (self-service) Knowledge Articles and videos. As written in the “Bi-Annual Review Process”, this shall include contacting subject matter experts (SMEs) to determine the disposition of the Articles. The Subject Matter Expert (SME) of the article shall determine if the article need to be extended an additional six months, update or retired. |
|  | The Contractor shall select a Team Manager with proven, documented experience working in a knowledge management department or organization. A certification from a reputable knowledge management organization, such as the Knowledge Management Institute or Association for Talent Development, is preferred. |
|  | The Contractor shall select contractor personnel with a minimum of three (3) years’ proven, documented professional experience in the knowledge management field, written communication, editing, technical documentation, and equivalent functional area expertise for their respective Services. |
|  | The Contractor shall incorporate VA approved best practices in system design to minimize the burden of maintaining the required knowledge repositories and maximize its effectiveness. |
|  | The Contractor shall work with designated Subject Matter Experts (SMEs) to track this process to validate articles and perform updates, retirements, and revisions as indicated |
|  | The Contractor shall provide a detailed weekly status report due by 12 noon Eastern every Friday that lists the following information from the previous week: All Knowledge Articles created, updated, and retired; all videos created and revised; article usage and viewed data. The status report shall also include a graph depicting the following information from the fiscal year start to present date: Article usage, number of articles attached to tickets, number of articles created, and videos produced. |
|  | The Contractor shall provide a weekly volume report depicting individual and team efforts. This report will address ticket distribution and completion efforts, as well as the number of Knowledge Articles attached to tickets. Create a ticket volume report within the ServiceNow (SNOW) or another VA/OIT specified platform. |
|  | The Contractor shall provide weekly and monthly Ticket Closure Reports depicting the number of tickets closed, number of tickets closed with Knowledge Article attachments, and tickets closed without Knowledge Article attachments. |
|  | The Contractor shall ensure editorial excellence and quality of all Knowledge Articles, delivering publish-ready Knowledge Articles with no errors in grammar, punctuation, or style. The Contractor shall ensure that all editorial components of Knowledge Articles comply with documented VA conventions and standards. Where conventions and standards are not documented by VA, the Contractor shall identify, document, and present recommendations for editorial consistency and excellence across Knowledge Articles. |
|  | The Contractor shall conduct a Critical Analysis of the Tier 0 and Tier 1 Knowledge Management program that is measured against Knowledge Management objectives, performance, and industry best practices, annually. The report shall contain an executive summary, description of analysis, scope, methodology, observations, and recommendations. The deliverable will not exceed twenty-five (25) pages (exclusive of appendices and references). The report shall be provided to the VA Knowledge Management Team by no later than September 30th each year. |
|  | The Contractor shall conduct monthly meetings throughout the period of performance. |
|  | The Contractor shall develop and provide a weekly Knowledge Management Accomplishments and Milestones report to VA. The document shall be distributed electronically and contain Accomplishments, Submissions, Number of Self-Service Views, First Contact Resolution (FCR) Percentage, Total Articles, Number of Video Created and Views for Each, and Top 20 Used Knowledge Articles. |
|  | The Contractor shall assist VA with the promotion of the Knowledge repositories housed in the search portal. This shall include presentations, marketing collateral, videos, talking points, articles, blog posts, etc. These promotional activities and collateral will be used to help customers find Knowledge Articles that resolve issues independently. |
|  | The Contractor shall provide their own training and written standard operating procedures during the transition period. |
|  | The Contractor shall meet with the VA Process Integration Team during onboarding meetings to ensure Tier 1 Knowledge Articles are created, updated, and retired as required. |
|  | The Contractor shall ensure the quality of the knowledge repository and thereby earn and retain user trust, by conducting a bi-annual (six months) review of knowledge articles based on their published dates. |
|  | The Contractor shall complete all submission requests within five business days by delivering publish-ready Knowledge Articles, sequencing work based on priority and impact. If the Contractor makes three attempts to contact SMEs and does not receive a response, the Contractor shall elevate the submission request to the VA ESD Knowledge Management Team before the end of the 5-day response period. |
|  | The Contractor shall identify a VA SME for each Knowledge Article housed in Tier 0 (Self-Service) and Tier 1 repositories based on a master repository provided by VA. SMEs exclude contract staff. If a SME is not identified, the request will be elevated to the VA Knowledge Management Team. |
|  | The Contractor shall create and maintain a checklist to include Title, KA Number, FCR (yes or no), Overview, Technical Action, and Solution. for each Knowledge Article entered in the Tier 0 (self-service) and Tier 1 repositories. |
|  | The Contractor shall perform an Article Quality Index (AQI) check for each Knowledge Article before it is placed in the Tier 0 (self-service) and Tier 1 repositories. |
|  | The Contractor shall provide a quality checklist and the quality check process to the ESD Knowledge Management Team and stored online (e.g., SharePoint, etc.) for the KM Team to access. |
|  | The Contractor shall document and record all meetings attended and store the documentation online (e.g., SharePoint, etc.) for the Knowledge Management Team to access. |
|  | The Contractor shall inform, discuss, and obtain written approval from the VA Knowledge Manager for all major changes to processes, procedures, repositories, etc. before implementation. |
|  | The Contractor shall provide ad hoc reports regarding Tier 0 (self-service) and Tier 1 Articles upon request. |
|  | All reports delivered by the Contractor shall not exceed twenty-five (25) pages (exclusive of appendices and references). |
|  | The Contractor shall provide weekly and monthly Submissions Reports depicting the number of submissions, and the number of Knowledge Article created from submissions. The report shall also include the number of submissions assigned to analysts and the number of submissions closed during the specified time period. |
|  | The Contractor shall ensure the quality of the knowledge repository and thereby earn and retain user trust, by conducting a bi-annual (six months) review of knowledge articles based on their published dates. |
|  | When updating or creating a Knowledge Article or completing a Submission request, the Contractor shall document and place explicit action notes in the portal. |
|  | The Contractor shall provide a monthly detailed status report of all KM activities, accomplishments, number of Knowledge articles created, operational metrics to include the number of videos created the number of submissions (assigned, unassigned, draft/checked out, In review, No SME, etc.), and explain how the work was performed and achieved a Knowledge Management/OIT/VA goal(s). This report and presentation shall be provided to VA two (2) business days prior to the meeting. The deliverable will not exceed twenty-five (25) pages (exclusive of appendices and references). |
|  | The Contractor shall work with the designated Subject Matter Experts (SMEs) to track and validate articles. When a new SME is added, the Contractor shall contact VA Knowledge Management to ensure a new SME Dashboard for the expert. The Contractor shall also perform updates, retirements, and revisions as indicated by the SME. |

**Deliverables:**

1. Knowledge Articles
2. Instructional Self-Service Videos with Audio, Visual, and Closed Caption Components
3. Knowledge Articles Weekly Report
4. Knowledge Submission Closure Reports
5. Critical Analysis Report
6. Weekly Accomplishment and Milestones Report
7. Ad Hoc Reports

## OPTIONAL TASK One -SPANISH SPEAKING OPTION

The tables below contain detailed descriptions requirements relating to the Spanish Speaking telephony services. This Optional Task may be exercised once per base and each option period, totaling five times. Normal ticket response and processing time applies as outlined in section 6.1 Performance Metrics.

|  |  |
| --- | --- |
|  | **Spanish Speaking Service Operations** |
|  | Vendor will provide Spanish Speaking services via all established contact channels with the exception of self-service tickets. . |
|  | Handle/triage requests in accordance with standard operating procedures and Service Level Agreement thresholds. |
|  | Document actions and/or customer interactions related to Incidents and Requests via all established contact channels with the exception of self-service tickets in ITSM Tool. |

## OPTIONAL TASK Two – TRANSITION OUT

### 5.8.1 TRANSITION-OUT TEAM AND REQUIREMENTS PLANNING

If exercised, at the commencement of Transition-out Service period, the Contractor shall appoint a Project Manager for Transition-out Services. The Contractor shall identify and document all open items during the Transition-out, determine a Resolution date and obtain VA concurrence for any items that will not be closed prior to completion of the Transition-out. The Contractor shall support the Transition-out period; and provide on-site support to facilitate parallel Transition-out and operations activities.

5.8.2**TRANSITION-OUT PLAN**

The Contractor shall provide an orderly Transition-out of work acceptance and accomplishment so that impact to the Services is minimal. Interruptions or delays to the work will adversely impact the mission. Therefore, the Contractor shall provide maximum cooperation with the successor while ensuring that no work receives inadequate attention during phase-out. The Contractor shall plan for a six (6) month Transition-out period of work, to ensure continuity of Services during the phase-out period.

At the conclusion of this contract, the Contractor shall ensure a smooth transition during the successor’s phase-in period. The Contractor shall aid the successor in the development of plans, procedures, and methods for assumption of all on-going work. The Contractor shall provide an orderly Transition-out of work acceptance and accomplishment, so that full control by the successor 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 PWS, as well as the existing PPM, and delivery of baseline metrics and statistics. The Contractor shall develop a Transition-out Plan for Government approval.

The Contractor shall undertake the Transition-out plan to facilitate the successful transfer of operational responsibility for the Services. This Transition-out Plan shall include, but is not limited to:

1. The key activities and expected results
2. The transition out acceptance criteria that shall be approved by VA
3. The data for the stages linked to such results
4. An outline of how the Contractor intends to work with VA or VA’s designee(s) to ensure an orderly transfer of the Services (the risks considered shall be clearly stated and an explanation shall be provided for how the Contractor’s solution and approach will reduce the impact of these risks)
5. Requirements for collaboration with VA or VA’s designee(s) to ensure an orderly Transition-out of the Services
6. Roles and responsibilities of the Contractor during the Transition-out Services period. The description of the Transition-out for each function, including the methodology for the transfer of knowledge between the Contractor’s personnel and the personnel who will be responsible for providing the Services in the future
7. Identification of risks in the transfer process, risk minimization strategies, and preventive measures
8. How the quality and level of the Services and the Service Levels will be achieved during the Transition-out Services period
9. Address security, Disaster Recovery (DR), and Business Continuity (BC) planning during the Transition-out Services period
10. Process description from the Contractor as to how access to critical infrastructures and Equipment is limited to Authorized Personnel
11. Description from the Contractor as to how insufficiently documented Systems and Equipment are treated
12. Designation of the rooms utilized by the Contractor within VA
13. Description of Change and release management, including all approvals and certifications by VA
14. As part of the Transition-out Plan, the Contractor shall submit a proposed diagram of how the transfer of the Services will be organized
15. The Contractor’s description of the process for checking the Transition-out Plan, including the terms which state that VA may monitor such process
16. Transition of all historic data to new successor System.
17. Transfer of all necessary business and/or technical Documentation relating to, but not limited to, standard operating procedures (SOPs), processes, plans, knowledge base, FAQs, PPM, and training.
18. Methodology of retaining personnel during transition period
19. Transfer of all incoming Contact channels including telephone numbers, email addresses, WebChat URL, to the successor or to the VA, as designated by VA.
20. Turn-in of all Government keys, ID/access cards, security tokens, and security codes.
21. Transition and/or transform the Services with no or minimal disruption or degradation of Services to VA.

Until the Transition-out Plan is complete, the Contractor shall take action to update the Transition-out Plan, including the impacts of issues and risks which are identified by the Contractor and VA. The Contractor shall also propose changes to the Transition-out Plan when asked to do so by VA. Changes to the Transition-out Plan must be approved by VA in writing. The Contractor shall provide Daily, Weekly, and Monthly Transition Status Reports and maintain performance commitments during the Transition Period. The Transition Status Report shall provide a description of accomplishments and progress against Transition-Out Plan including next week’s activities, issues, risks, and risk mitigation approaches.

**Deliverables:**

1. Transition-Out Plan
2. Transition Status Report

## GENERAL REQUIREMENTS

## ENTERPRISE AND IT FRAMEWORK

6.1.1 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.

### 6.1.3INTERNET 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.

### 6.1.4 TRUSTED INTERNET CONNECTION (TIC)

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

### STANDARD COMPUTER CONFIGURATION

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

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

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

### PROCESS ASSET LIBRARY (PAL)

The Contractor shall perform their duties consistent with the processes defined in the OIT Process Asset Library (PAL).  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

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

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

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

| **Task Number** | **Tier1 / Low Risk** | **Tier 2 / Moderate Risk** | **Tier 4 / High Risk** |
| --- | --- | --- | --- |
| 5.1 |  |  |  |
| 5.2 |  |  |  |
| 5.3 |  |  |  |
| 5.4 |  |  |  |
| 5.5 |  |  |  |
| 5.6 |  |  |  |
| 5.7 |  |  |  |
| 5.8 |  |  |  |

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

### CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

**Contractor Responsibilities:**

1. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
2. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor’s Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
3. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
4. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
5. Optional Form 306
6. Self-Certification of Continuous Service
7. VA Form 0710
8. Completed SIC Fingerprint Request Form
9. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management’s (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
10. The Contractor employee shall certify and release the e-QIP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
11. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. 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

## 6.3 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 paragraphs below define the performance standards and acceptable levels of performance associated with this effort. In addition to the performance metrics set forth below, 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.

### SERVICE LEVEL FRAMEWORK

This section sets forth the functional and technical specifications for the Critical Performance Indicators (CPI), and Key Performance Indicators (KPI) to be established between the Contractor and VA. This section contains the tables and descriptions that provide VA framework and expectations relating to Service Level commitments, and the implications of meeting versus

failing to meet the requirements and objectives, as applicable. This section defines VA detailed performance, management, and reporting requirements for Contractor Services.

The method set out herein will be implemented to manage the Contractor’s performance against each Service Level in order to monitor the overall performance of the Contractor. The PWS shall be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this PWS:

* Service Level Specific Performance – Agreed upon specific Service Level Agreements (SLAs) to measure the performance of specific Services or Service Elements.
* Overall PWS Performance – An overall Contractor performance score across all Service Levels (i.e., CPI and KPI). The overall performance score is linked to Governance and escalation processes as needed to initiate corrective actions and remedial processes.

### ASSESSMENT FOR MISSED SERVICE LEVELS

The Service performance metrics are directly related to the Service Level requirements set forth below. The Contractor is required to meet all requirements established by this PWS. However, if the Contractor’s performance falls below a required Service Level, the Contractor shall only be paid for the lower level provided Service Level. The VA’s payment for the lower Service Level provided in no way waives the Government’s right to pursue any remedies available by law, including, but not limited to, termination for default. VA will begin assessing lower Service Level prices for all CPIs as described in Section 6.1.3, commencing with the fifth month of TO performance. The COR will notify the Contractor and CO in writing when any CPI metric has been missed.

The first month a CPI metric is missed, the Contractor will be assessed a ten percent (10%) lower price against the applicable CLIN(s) for that month. Each consecutive month a metric is missed, the Contractor will be assessed a ten percent (10%) lower price against the applicable CLIN(s). If multiple metrics are missed, then the Contractor will be assessed the applicable lower price for each metric missed. For example, if the Contractor misses CPIs for the Incident Resolution Time and Service Request Fulfilled Time within Service Level metrics during the sixth month of performance, then the Contractor shall be assessed a ten percent (10%) price reduction against the applicable CLIN(s), as it has provided a lower than agreed to Service Level for two (2) CPI metrics.

Prices for lower Service Levels will be assessed against the CPI metrics only as described in Section 6.1.3. If a lower Service Level is assessed in a particular month, the Contractor shall provide an itemized invoice detailing the lower Service Level price (percentage and amount) and deducting that lower Service Level price from the total monthly cost of the applicable PWS Line Item Number in the following month’s invoice.

**Prices for Lower Service Levels for missed metrics:**

* First month missed per CPI metric = ten percent (10%) price reduction for lower Service Levels
* Each consecutive month missed per CPI metric = ten percent (10%) price reduction for lower Service Levels

### SERVICE LEVEL REQUIREMENTS

The Contractor shall meet the Service Level requirement for each Service Level which identifies the calculation and measurement of each Service Level. The Service performance indicator type and support hour requirement is specified in the table below.

“Critical Performance Indicators” or “CPIs” means those Service Levels that are described in PWS as a CPI.

“Key Performance Indicators” or “KPIs” means those Service Levels that are described below as a KPI.

For clarity, in the event of lower service levels the Contractor’s payment will not be reduced for the Service Levels until completion of the TIER 1 Service Transfer Phase as specified in paragraph 5.3.

| Acronym/ How Measured | Metric/ Definition/ Calculation and Notes | | Service Level | | Measurement Window | | Reporting Window | Acceptable Quality Level (AQL) of Performance | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1: FCR – T1** | **First Contact Resolvable (Tier-1)** | | KPI | | Monthly | | Monthly | Greater than 95%; see Note 1 below | |
| Percentage of Incident Tickets Resolved on the first Contact (including **all** PIV exemption request tickets)  (Does not include Contacts which are not resolvable by the ESD.) | Measures the percent of Incident Tickets originating from Contacts Resolved during the first End User Contact determined to be Resolvable at the Tier 1 level as determined by the respective knowledge article for the issue presented. | | | | | | | | |
| Contacts which by their nature cannot be Resolved during the initial Contact, as determined by the respective knowledge article for the issue presented, shall be excluded from this calculation. | | | | | | | | |
| **2: ASA** | **Response Time**  **- Average Speed to Answer** | | CPI | | Monthly | | Monthly | ≤150 seconds | |
| The timing for answering the Contact begins when the Contact is queued on the ACD queue and ends when an agent (either in the primary or overflow ACD queue) responds to the Contact. | The Average Speed of Answer for contacts received by an ACD queue. | | | | | | | | |
| The timing for responding to the Contact begins when the Contact is queued in the ACD queue and ends when an agent (either in the primary or overflow ACD queue) responds to the Contact.  Target response time is ≤ 150 seconds.  Note: Contacts will include all mediums, current and future state (e.g., calls, LiveChat, SMS/text and self-service tickets) | | | | | | | | |
| **3: ASA Compliance** | **Response Time – Average Speed to Answer Compliance** | | | KPI | | Monthly | Monthly | 85% | |
| The timing for answering the Contact begins when the Contact is queued on the ACD queue and ends when an agent (either in the primary or overflow ACD queue) responds to the Contact. | The percentage of contacts, as measured on a contact-by-contact, basis meeting the ≤150 seconds CPI for ASA | | | | | | | | |
| The timing for answering the Contact begins when the Contact is queued on the ACD queue and ends when an agent (either in the primary or overflow ACD queue) responds to the Contact. The measure is done on a contact-by-contact basis to calculate the percentage of contacts that individually meet the ≤150 seconds threshold for ASA | | | | | | | | |
| **4: CAR** | **Contact Abandonment Rate** | | CPI | | Monthly | | Monthly | <5% | |
| Percentage of Contacts not answered after being added to the queue | Abandoned Contacts after being put into queue with the exception of those abandoned within the first 10 seconds of being put into the queue. | | | | | | | | |
|  | | | | | | | | |
| **5: DQ** | **Documentation Quality Metric** | | KPI | | Monthly | | Monthly | >95% | |
| Percentage of accurate Tier 0/Tier 1Knowledge Article system records | Contractor upkeep of Documentation in the Knowledge Article repository | | | | | | | | |
| For any given record category of a record, the lack of accuracy in any one attribute equates to the entire record being inaccurate. By using a specified quality management index – currently Article Quality Index (AQI) within the SNOW system – the VA will determine the overall accuracy via random sampling. | | | | | | | | |
| **6: CQ** | **Contact Quality** | | KPI | | Monthly | | Monthly | >90% | |
| Percentage of high-quality score contacts monitored by quality assurance | Average quality score of all Contacts taken by ESD that were monitored by independent Quality Assurance team. | | | | | | | | |
| Note: Independent Quality Assurance team conducts an assessment of the quality of the ESD services monthly by monitoring at least three phone calls and three chats (where applicable), per agent, each month, | | | | | | | | |
| **7: IResvlT – VIP** | **Incident Resolution Time - VIP End User** | | KPI | | Monthly | | Monthly | >99% | |
| Percentage of VIP End User Incidents (All Priorities) that are Resolved within the Expected (Targeted) Service Level. | Percentage of VIP First Contact Resolvable End User Incidents (all Priorities) that are Resolved within one (1) Hour during the Measurement Window. | | | | | | | | |
|  | | | | | | | | |
| **8: IResplT – VIP** | **Incident Response Time- VIP End User** | | KPI | | Monthly | | Monthly | >99% | |
| Percentage of VIP End User Incidents that are Responded to within 15 minutes. | Percentage of VIP End User Incidents (all Priority) that are Responded to within 15 minutes during the Measurement Window. | | | | | | | | |
| Measures the time to Respond. | | | | | | | | |
| **9: CT** | **End User Service Satisfaction - Closed Tickets** | | CPI | | Monthly | | Monthly | ≥4.5 | |
| All post-call surveys provided by the Automated Call Distribution system returned with an average score (of the questions asked and answered) at or above the defined Service Level. | End User satisfaction post-call surveys have an average satisfaction response rating of ‘4.5' or higher. | | | | | | | | |
| Response of surveys Scale 1 to 5:  1 = Very Dissatisfied, 2 = Dissatisfied, 3 = Neutral, 4 = Satisfied, 5 = Very Satisfied. | | | | | | | | |
| **10: CT SNOW** | **End User Service Satisfaction** | KPI | | | | Monthly | Monthly | ≥4.25 | |
|  | End User satisfaction surveys have an average satisfaction response rating of ‘4.25' or higher. | | | | | | | | |
| Response of surveys Scale 1 to 5:  1 = Very Dissatisfied, 2 = Dissatisfied, 3 = Neutral, 4 = Satisfied, 5 = Very Satisfied. | | | | | | | | |
| **10: PI** | **Process Integration** | | | KPI | | Monthly | Monthly | | 5 business days |
| Completed and approved process flow documentation for Tier 1 support on new or updated applications, platforms, and programs | Process flow documentation and approval elapsed time | | | | | | | | |
| Completed and approved process flow documentation for Tier 1 support on new or updated applications, platforms, and programs. The measure is the elapsed time for completion and approval of documented process flows once all parties (VA, Tier 1 vendor and SME) are in agreement on the process flow for the specific application, platform, or program. | | | | | | | | |
| **11: KM** | **Knowledge Management** | | | KPI | | Monthly | Monthly | | 5 business days |
| Completion of all submission requests for new knowledge articles or updates to existing knowledge articles | Knowledge Article submission completion elapsed time | | | | | | | | |
| The Contractor shall complete all submission requests within five business days by delivering publish-ready Knowledge Articles, sequencing work based on priority and impact. The measurement is the elapsed time for delivery of publish-ready knowledge articles once all parties (VA and Tier 1 vendor) are in agreement on the content of the knowledge article. | | | | | | | | |

# 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. Physical Security & Safety Requirements:

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

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

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

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

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