PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS
Office of Information & Technology
Service Delivery and Engineering

Program Administration Office

Sustainment of Enterprise Voice System
Proof of Concept (EVS PoC) Sites

Date: May 7, 2015
TAC-15-21936
PWS Version Number: 1.0

Contents

1.0 BACKGROUND 5
2.0 APPLICABLE DOCUMENTS 6
3.0 SCOPE OF WORK 11
4.0 PERFORMANCE DETAILS 12
4.1 PERFORMANCE PERIOD 12
4.2 PLACE OF PERFORMANCE 12
4.3 TRAVEL 13
5.0 SPECIFIC TASKS AND DELIVERABLES 14
5.1 PROJECT MANAGEMENT 14
5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN 14
5.1.2 PROJECT KICKOFF MEETINGS 15
5.1.3 REPORTING REQUIREMENTS 15
5.1.4 BRIEFINGS 16
5.2 CONTRACT TRANSITION 16
5.2.1 TRANSITION-IN SUPPORT SERVICES (OPTIONAL TASK) 16
5.2.2 TRANSITION- OUT SUPPORT SERVICES (OPTIONAL TASK) 17
5.3 OPERATIONS, MAINTENANCE, ADMINISTRATION, PROVISIONING, AND REPAIR (OMAPR) 18
5.3.1 OMPAR REPORTS 18
5.3.2 SERVICE DESK & TECHNICAL SUPPORT 19
5.3.3 EVS PoC ADMINISTRATION 32
5.3.4 BUILD AND RELEASE MANAGEMENT 38
5.3.5 CHANGE, CONFIGURATION AND ASSET MANAGEMENT 40
5.3.6 PERFORMANCE MANAGEMENT 45
5.3.7 SECURITY MANAGEMENT 47
5.3.8 KNOWLEDGE MANAGEMENT 56
5.4 OPTIONAL TASKS 56
5.4.1 OPTIONAL: MACD LOCAL LEVEL SUPPORT 56
5.4.2 OPTIONAL: SITE ACTIVATION SUPPORT 56
5.4.3 OPTIONAL: MOVE VOICEMAIL FROM CORES TO SITES 57
5.4.4 OPTIONAL: CORE AND DISTRIBUTION LAYER EXPANSION SUPPORT 57
5.4.5 OPTIONAL: CONVERGED VIRTUAL INFRASTRUCTURE 58
5.4.6 OPTIONAL: ACTIVITIES SUPPORTING INTEGRATION WITH IPv6 58
5.4.7 OPTIONAL: INTEGRATION WITH VA ENTERPRISE UC APPLICATIONS 59
5.4.8 OPTIONAL: INCREMENTAL EQUIPMENT PURCHASE 60
5.4.9 OPTIONAL: CAPACITY AUGMENTATION 60
5.4.10 OPTIONAL: DATABASE ADMINISTRATION 60
6.0 GENERAL REQUIREMENTS 62
6.1 ENTERPRISE AND IT FRAMEWORK 62

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 65
6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 65
6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS 67
6.3 METHOD AND DISTRIBUTION OF DELIVERABLES 68
6.4 PERFORMANCE METRICS 69
6.5 FACILITY/RESOURCE PROVISIONS 73
6.6 GOVERNMENT FURNISHED PROPERTY 73
ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED 74
ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE 81
ADDENDUM C – EVS PoC LOCATION ADDRESSES 116
VA CENTRAL OFFICE 116
VA CORE SITES 116
SUPPORT SITES 116
PRIMARY SITES 116
VA Montana Health Care System 116
Ralph H. Johnson VA Medical Center, Charleston, SC 118
Tennessee Valley Healthcare System 118
ADDENDUM D – EVS PoC TECHNICAL REQUIREMENTS 120
D.1.0 EVS PoC SERVICE LEVEL AGREEMENT (SLA) 120
D.1.1 NSD PRIORITY MATRIX 120
D.1.2 SYSTEM PERFORMANCE, MONITORING, AND REPORTING 122
D.1.3 AVAILABILITY 123
D.1.4 NETWORK, LINK, AND INFRASTRUCTURE AVAILABILITY 124
D.1.5 EFFECTIVE DATE 125
D.2.0 USER PROFILES 125
D.3.0 OPERATOR AND E911 SERVICES 126
D.4.0 EMERGENCY RESPONSE SERVICES REQUIREMENTS 127
D.5.0 HOTLINES 127
D.7.0 CODEC AND PROTOCOL SUPPORT 127
D.8.0 AUTOMATIC CALL DISTRIBUTION (ACD) AND INTERACTIVE VOICE RESPONSE (IVR) CAPABILITIES 128
D.9.0 ANALOG SERVICES 141
D.10.0 SOFT PHONES 141
D.11.0 DIAL PLAN 141
D.12.0 LONG DISTANCE AUTHORIZATION 142
D.13.0 CALL DETAIL RECORDS (CDR) 142
D.14.0 ADDITIONAL GENERAL VOICE FEATURES 143
ADDENDUM E – SUPPLEMENTARY INFORMATION 148
E.1.0 LIST OF VA TOOLS AVAILABLE FOR MANAGEMENT, MONTIORING, AND REPORTING 148
E.2.0 ACRONYMS 148
E.3.0 DEFINITIONS 155
ADDENDUM F – SECTION C CONTRACT CLAUSES 169
C.1.0 FSS RFQ INTRODUCTORY LANGUAGE 169

C.2.0 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 169
C.3.0 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (FEB 2012) 169
C.4.0 52.217-7 OPTION FOR INCREASED QUANTITY--SEPARATELY PRICED LINE ITEM (MAR 171
1989) 171
C.5.0 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000) 171
C.6.0 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008) 171
C.7.0 FAR 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION) (AUG 2012) 171
C.8.0 VAAR 852.203-71 DISPLAY OF DEPARTMENT OF VETERAN AFFAIRS HOTLINE POSTER (DEC 1992) 172
C.9.0 VAAR 852.215-70 SERVICE-DISABLED VETERAN-OWNED AND VETERAN-OWNED SMALL BUSINESS EVALUATION FACTORS (DEC 2009) 172
C.10.0 VAAR 852.215-71 EVALUATION FACTOR COMMITMENTS (DEC 2009) . 172
C.11.0 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008) 173
C.12.0 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012) 173
C.13.0 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984) 174
ADDENDUM G – LIST OF ATTACHMENTS 175
Attachment 1 - SDE PAO Meeting Agenda Template 175
Attachment 2 - SDE PAO Meeting Notes Template 175
Attachment 3 - VA UC TRM National Dial Plan 175
Attachment 4 - EVS PoC Technical Support Tier Matrix 175
Attachment 5 - Configuration Management Plan Template 175
Attachment 6 - Field Operations Change Management SOP 175
Attachment 7 - National Change Process (Normal) 175
Attachment 8 - National Change Process 176
Attachment 9 - National Change Process - Patching 176
Attachment 10 - National Change Management Escalation Process 176
Attachment 11 - OIT Availability Management Process 176
Attachment 12 - OIT Capacity Management Process 176
Attachment 13 - OIT Change Management Process 176
Attachment 14 - OIT Configuration Management Process 176
Attachment 15 - OIT Event Management Process 176
Attachment 16 - OIT Incident Management Process 177
Attachment 17 - OIT Knowledge Management Process 177
Attachment 18 - OIT Problem Management Process 177
Attachment 19 - OIT Release Management Process 177
Attachment 20 - OIT Request Fulfillment Management Process 177
Attachment 21 - Patch Management and Compliance Memorandum 177
Attachment 22 - Patch Management Flow Chart 177
Attachment 23 - Quarterly Change Order Review SOP 177
Attachment 24 - SDE Change Managment Plan 178

Attachment 25 - SDE Change Management Plan for National Patch Mgmt 178
Attachment 26 - SDE National Change Control Board SOP 178
Attachment 27 - Security Impact Analysis Template 178
Attachment 28 - EVS PoC Cores (Austin & Hines) Inventory List 178
Attachment 29 - Fort Harrison Inventory List 178
Attachment 30 - Contractor Project Management Plan Template - Pending 178
Attachment 31 - EVS PoC System Security Plan - Pending 179
Attachment 32 - EVS Helpdesk Procedure Documents - Multiple Pending 179
Attachment 33 - List of National VA Support Contracts - Pending 179
Attachment 34 - ScienceLogic Inventory List - Pending 179
Attachment 35 - Tennessee Valley Inventory List - Pending 179
Attachment 36 - Charleston Inventory List - Pending 179
ADDENDUM H – PoC ARCHITECTURE 180

1.0 BACKGROUND

The mission of the Department of Veterans Affairs (VA), Office of Information and Technology (OI&T), Service Delivery and Engineering (SDE), Enterprise Systems

Engineering (ESE), and Office of Information Security (OIS) is to support providing benefits and services to Veterans of the United States. In meeting these goals, OI&T strives to provide high quality, effective, and efficient Information Technology (IT) services to those responsible for providing care to the Veterans at the point-of-care as well as throughout all the points of the Veterans' health care in an effective, timely and compassionate manner. VA depends on Information Management/Information Technology (IM/IT) systems to meet mission goals.

The focus of the Contractor requirements specified in this PWS is the delivery of a unified and centrally managed voice services capability, addressing the issues with aging, legacy private branch exchange (PBX) systems at VA's facilities and current gaps in the contact center functionality used in direct telephonic interaction with our Veterans. Legacy is defined as those systems which are currently in place, are aged, Time-Division Multiplexing (TDM) technology, or may require upgrades to meet the Voice over Internet Protocol (VoIP) delivered as part of the Enterprise Voice System Proof of Concept (EVS PoC) project. VA deployed a Proof of Concept (PoC) for the Enterprise Voice System (EVS) that provides voice services to locations within the Montana Healthcare System, Tennessee Valley Healthcare System, and locations associated with the Ralph H. Johnson Medical Center in Charleston, SC. A high-level diagram depicting the EVS PoC architecture is included in Addendum H. The work described in this PWS provides Operations, Maintenance, Administration, Provisioning, and Repair (OMAPR) of these systems.

2.0 APPLICABLE DOCUMENTS

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

1. 44 U.S.C. § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
8. VA Directive 0710, "Personnel Suitability and Security Program," June 4, 2010, http://www1.va.gov/vapubs/
9. VA Handbook 0710, Personnel Suitability and Security Program, September 10, 2004, http://www1.va.gov/vapubs/

10. VA Directive and Handbook 6102, “Internet/Intranet Services,” July 15, 2008
11. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
12. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
13. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
14. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
15. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
16. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
17. VA Directive 6500, “Managing Information Security Risk: VA Information Security Program,” September 20, , 2012
18. VA Handbook 6500, “Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,” September 20, 2012
19. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
20. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI)”, January 6, 2012
21. VA Handbook 6500.3, “Assessment, Authorization, And Continuous Monitoring Of VA Information Systems,” February 3, 2014
22. VA Handbook, 6500.5, “Incorporating Security and Privacy in System Development Lifecycle” March 22, 2010
23. VA Handbook 6500.6, “Contract Security,” March 12, 2010
24. Project Management Accountability System (PMAS) portal (reference https://www.voa.va.gov/pmas/)
25. OI&T ProPath Process Methodology (reference https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=27) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
26. Technical Reference Model (TRM) (reference at http://www.va.gov/trm/TRMHomePage.asp)
27. National Institute Standards and Technology (NIST) Special Publications (SP)
28. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
29. VA Directive 6300, Records and Information Management, February 26, 2009
30. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
31. OMB Memorandum, “Transition to IPv6”, September 28, 2010
32. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, February 17, 2011
33. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 20, 2014

34. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
35. 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
36. OMB memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
37. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
38. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
39. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
40. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
41. NIST SP 800-63-2, Electronic Authentication Guideline, August 2013
42. Draft NIST Special Publication 800-157, Guidelines for Derived PIV Credentials, March 2014
43. NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
44. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
45. 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)
46. VA Memorandum, VAIQ # 7011145, VA Identity Management Policy, June 28, 2010 (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
47. 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)
48. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, October 1, 2013
49. OMB Memorandum M-08-05, “Implementation of Trusted Internet Connections (TIC), November 20, 2007
50. OMB Memorandum M-08-23, Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008
51. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)

52. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
53. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
54. Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” October 5, 2009
55. Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” January 24, 2007
56. Executive Order 13221, “Energy-Efficient Standby Power Devices,” August 2, 2001
57. VA Directive 0058, “VA Green Purchasing Program”, July 19, 2013
58. VA Handbook 0058, “VA Green Purchasing Program”, July 19, 2013
59. 44 U.S.C. § 3541, “Federal Information Security Management Act (FISMA) of 2002”
60. Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements For Cryptographic Modules”
61. FIPS Pub 201, “Personal Identity Verification of Federal Employees and Contractors,” March 2006
62. 10 U.S.C. § 2224, "Defense Information Assurance Program"
63. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level2 procedures and processes
64. 5 U.S.C. § 552a, as amended, “The Privacy Act of 1974”
65. 42 U.S.C. § 2000d “Title VI of the Civil Rights Act of 1964”
66. Department of Veterans Affairs (VA) Directive 0710, “Personnel Suitability and Security Program, “May 18, 2007
67. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
68. 36 C.F.R. Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
69. OMB Circular A-130, “Management of Federal Information Resources,” November 28, 2000
70. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
71. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
72. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
73. Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004
74. VA Directive 6500, “Information Security Program,” September 20, 2012
75. VA Handbook 6500, “Information Security Program,” September 2012
76. VA Handbook 6500.1, “Electronic Media Sanitization,” March 22, 2010
77. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI),” January6, 2012.
78. VA Handbook 6500.3, “Certification and Accreditation of VA Information Systems,” November 24, 2008.

79. VA Handbook, 6500.5, “Incorporating Security and Privacy into the System Development Life Cycle”, March 22, 2010
80. VA Handbook 6500.6, “Contract Security,” March 12, 2010
81. Project Management Accountability System (PMAS) portal (reference PWS References –Technical Library at HYPERLINK "https://www.voa.va.gov/" \h https://www.voa.va.gov/)
82. OI&T ProPath Process Methodology (reference PWS References - Technical Library and ProPath Library links at HYPERLINK "https://www.voa.va.gov/" \h https://www.voa.va.gov/) NOTE: In the event of a conflict, OI&T ProPath takes precedence over other processes or methodologies.
83. Technical Reference Model (TRM) (reference at HYPERLINK "http://trm.oit.va.gov/TRMHomePage.asp" \h http://trm.oit.va.gov/TRMHomePage.asp, or HYPERLINK "https://www.voa.va.gov/" \h https://www.voa.va.gov/)
84. National Institute Standards and Technology (NIST) Special Publications
85. VA Directive 6508, VA Privacy Impact Assessment, October 3, 2008
86. VA Directive 6300, Records and Information Management, February 26, 2009
87. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
88. ITU-T P.1010, Fundamental Voice Transmission Objectives for VoIP Terminals and Gateways of the International Telecommunications Union (ITU)
89. NIST SP 800-58,-Security Considerations for Voice Over IP Systems
90. Recommendations of the National Institute of Standards and Technology (NIST)
91. TIA PN-3-027.562, VoIP Supplementary Services Descriptions of the Telecommunications Industry Association (TIA)
92. TIA TIA-811-A, Telecommunications Performance and Interoperability Requirements for VoIP Features
93. VA Handbook 6500, “Risk Management Framework for VA Information Systems Tier 3: VA Information Security Program”
94. Joint Commission on Accreditation of Healthcare Organizations (The Joint Commission) standards http://www.gao.gov/new.items/d06826.pdf
95. NIST SP 800-34, Contingency Planning Guide for Federal Information Systems
96. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
97. Federal Continuity Directive (FCD) -1
98. National Security Presidential Directive 51 (NSPD-51), May 4, 2007
99. Homeland Security Presidential Directive 20 (HSPD-20), May 4, 2007
100. Federal Information Security Management Act (FISMA)
101. National Continuity Policy Implementation Plan
102. National Response Framework
103. VA Directive 0320, VA Comprehensive Emergency Management Program
104. VA Handbook 0320, Comprehensive Emergency Management Program

105. VA Handbook 0322.1, VA Integrated Operations Center
106. VA Directive 0324, Test, Training, Exercise, and Evaluation Program
107. VA Handbook 6500.8, Information System Contingency Planning
108. NFPA 70: National Electrical Code ®, 2014 Edition, published by the National Fire Protection Association
109. NFPA 99: HealthCare Facilities Code, 2015 Edition, published by the National Fire Protection Association
110. NFPA 101: Life Safety Code®, 2015 Edition, published by the National Fire Protection Association
111. NFPA 110: Standard for Emergency and Standby Power, 2013 Edition, published by the National Fire Protection Association
112. VA Network and Computing standards to be provided at award
113. NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
114. NIST SP 500-267, A Profile for IPv6 in the U.S. Government, July 2008
115. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
116. 19 U.S.C. § 2501, “Trade Agreements Act”
117. VA Memorandum “Server Virtualize First Policy (VAIQ 7266972), August 27, 2012
118. VA Baseline Configuration Standard for Server Virtualization, v1.0, June 25,2012
119. VA Baseline Configuration Standard for VMware Guest Virtual Machines, v1.0, November 29, 2013
120. VA Baseline Configuration Standard for VMware vCenter 5.5, v1.0, November 29, 2013
121. VA Baseline Configuration Standard for VMware vSphere (ESXi) , v1.0, November 29, 2013
122. VA OI&T SDE “A High Level Strategic Management View: Communications Architecture and Infrastructure Modernization (2011-2016)”, v1.0, July 5, 2011
123. VA OI&T SDE “Communications Architecture and Infrastructure Modernization (2012-2016) Executive Summary”, Draft v2.2, November 28, 2011
124. ITIL, 2011 Edition

3.0 SCOPE OF WORK

The Contractor shall operate, maintain, administer, provision, and repair VA’s EVS PoC Proof of Concept. The Contractor also shall augment the existing EVS PoC architecture as needed to support capacity needs at existing EVS PoC locations, and transition of voicemail services from the EVS PoC core down to the site tier level. Detailed requirements regarding scope, specifications, and locations are provided in this PWS.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance shall be base period of one year from date of award, with four one-year options.

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO) or Contracting Officer's Representative (COR). Normal support activities shall occur during regular business hours unless otherwise required or negotiated with VA.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

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

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

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

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

4.2 PLACE OF PERFORMANCE

Tasks under this PWS shall be performed in VA facilities as specified in Addendum C.

Requirements for access to VA facilities shall include the following:

A. Typical working hours at VA facilities are 8:00 AM to 4:30 PM local time. Access after normal working hours shall be coordinated and approved with each site.
B. All contractors accessing VA facilities under this contract shall be required to obtain a VA Personal Identification and Verification (PIV) badge. Background investigation processing and badging takes approximately 60 days from time of submission request.

4.3 TRAVEL

The Government anticipates minimal travel to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences through the period of performance. Include all estimated travel costs in your firm fixed-price line items. These costs shall not be directly reimbursed by the Government.

Table 4.3 – 1: Travel Requirements.

Destination	Purpose	Number of People[3]	Number of Trips	Duration (Days)
Base Year				
Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC, 20420	Project Kickoff and Status Meetings	3	5	2
Austin Data Center, 1615 Woodward Street, Austin, TX 78772	Kickoff Meeting	2	1	2
Hines Data Center, 5000 South 5th Ave, Building 215, Hines, IL 60141	Kickoff Meeting	2	1	2
VA Montana Health Care System, VA Medical Center and Ambulatory Care Clinic, 3687 Veterans Drive, Fort Harrison, MT 59636	Kickoff and Status Meetings	3	2	2
Ralph H. Johnson VA Medical Center, 109 Bee Street, Charleston, SC 29401	Kickoff and Status Meetings	3	2	2
Tennessee Valley Healthcare System, Nashville Campus, 1310 24th Avenue South, Nashville, TN 37212	Kickoff and Status Meetings	3	2	3[1]
Tennessee Valley Healthcare System, Alvin C. York Campus, 3400 Lebanon Pike, Murfreesboro, TN 37129	Kickoff and Status Meetings	3	2	
Option 1 and Option 2[2]				
Washington, DC	Project Status Meeting	1	3	2
Austin, TX	Status Meeting	1	1	2
Hines, Il	Status Meeting	1	1	2
Ft. Harrison, MT	Status Meeting	1	1	2

Charleston, SC	Status Meeting	1	1	2
Nashville, TN	Status Meeting	1	1	2

Notes:

1. It is assumed that the main kickoff meeting will occur at the Nashville Campus, and that the members of the project management team making the trip will also visit the Alvin C. York Campus.
2. Travel is for each year, to the same locations as the base year.
3. The contractor may determine that more staff are necessary. Where possible, telepresence capabilities shall be leveraged for additional staff.

The Contractor may find it necessary to travel to some of the remote locations associated with the VAMCs. The names and addresses for all of the remote locations for each VAMC are listed in Addendum C.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor support service requirements specified in Section 5, apply to the PoC Architecture described in Addendum H.

The Contractor shall perform the following:

5.1 PROJECT MANAGEMENT

The contractor shall provide project management support under this contract. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a certified Program/Project Manager (PM), who shall provide management, direction, administration, quality control, and leadership of the execution of this contract. The Project Manager shall be provided a complete copy of this PWS, including all amendments, upon contract execution. The contractor shall schedule meetings and provide deliverables in accordance with this section.

Whenever possible, the contractor shall utilize VA templates for identified deliverables. If VA templates are not available, the contractor shall create templates that will be submitted to VA for review and approval.

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out in detail the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resources. The CPMP shall include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests and maintenance tasks as identified within the PWS. The initial baseline CPMP shall be concurred upon at project kick off and updated thereafter as required. The Contractor shall update and maintain the VA PM approved CPMP throughout the period of performance.

CPMP Template is attached in Addendum G.

Deliverables:

A. Contractor Project Management Plan (CPMP)

5.1.2 PROJECT KICKOFF MEETINGS

The Contractor shall host a Project Kickoff Meeting at a location approved by the VA. The meeting shall be coordinated with VA to take place within two weeks of contract award unless VA has extenuating circumstances preventing attendance. Any deviation from the two week window shall be approved by VA. The meeting will provide an introduction between the contractor personnel and VA program personnel who will be involved with the contract. The meeting will provide the opportunity to discuss technical, management, and security issues, on-boarding, travel, and reporting procedures. At a minimum, the attendees shall include key contractor personnel, the VA PM, COR, and CO. The contractor shall present the Project Kickoff Briefing at the Kickoff Meeting, as well as the draft CPMP.

Meeting Agenda and Minutes Template is attached in Addendum G.

Deliverables:

A. EVS PoC Sustainment Project Kickoff Meeting Agenda
B. EVS PoC Sustainment Project Kickoff Briefing
C. EVS PoC Sustainment Project Kickoff Meeting Minutes

5.1.3 REPORTING REQUIREMENTS

5.1.3.1 WEEKLY PROJECT STATUS UPDATES

At a minimum, a weekly status call shall be conducted with the VA PM, COR, and interested stakeholders. This conference call shall review project status, schedule, open action items, and any issues requiring discussion or notification. The Contractor shall provide the COR with a Weekly Status Report documenting key issues from the weekly status call. These reports shall reflect data as of the last business day of the preceding week. Weekly Status Reports shall be delivered weekly, beginning the first week after contract award. At a minimum, the weekly status report will address:

- Sustainment Project Status
- Sustainment Project Schedule
- Sustainment Project Risks and mitigations
- Summary of all tickets created and closed
- Detailed report of all Priority 1 tickets

Meeting Agenda and Minutes Template is attached in Addendum G.

Deliverables:

A. Weekly Status Call Agenda

B. Weekly Status Call Minutes

C. Weekly Status Report

5.1.3.2 MONTHLY PROGRESS AND PERFORMANCE REPORTS

The Contractor shall provide the VA PM and COR with Monthly Progress and Performance Reports in electronic form in Microsoft Word and Project formats. The report shall include detailed instructions/explanations for each data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding Month and will contain information on Contract, Technical and Service performance.

The Monthly Progress and Performance Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. The Contractor shall monitor performance against the CPMP and report any deviations from the original baseline and any contract modification of the schedule, to include monitoring and reporting. It is expected that the Contractor shall keep in communication with VA so that problems that arise are transparent to both parties to prevent escalation of outstanding issues.

Deliverables:

A. Monthly Progress and Performance Report

5.1.4 BRIEFINGS

The Contractor shall create and provide status via an Executive Leadership Briefing describing the EVS PoC Sustainment effort and supporting activities at a minimum of two briefings per month beginning 30 days after contract award. EVS PoC Sustainment project briefings shall be presented during kickoff meetings, prior to cutover, following cutover, and at other times as deemed appropriate or when requested by VA.

Deliverables:

A. Executive Leadership Briefing

5.2 CONTRACT TRANSITION

5.2.1 TRANSITION-IN SUPPORT SERVICES (OPTIONAL TASK)

The Contractor shall perform phase-in activities for transitioning services from legacy contractor at the end of their EVS PoC contract performance period. The Contractor shall include Phase-In Transition activities within the Transition Plan that describe the methodology, processes and phase-in activities. The Phase-In Transition Plan shall be delivered 14 days after contract award.

The Contractor shall provide phase-in support that includes the following steps:

a. Coordinating with contract phase-out activities;
b. Updating, validating, and transferring of inventory and support documentation;
c. Participating in phase-in transition activities

Deliverables:

A. Phase-In Transition Plan

5.2.2 TRANSITION- OUT SUPPORT SERVICES (OPTIONAL TASK)

The Contractor shall assist VA in the transition of EVS PoC services from the follow-on Contractor. The Contractor shall coordinate and transfer all EVS PoC management and technical data, such as site and desktop configurations, inventory, core and site(s) design diagrams and schematics. The Contractor shall comply with arrangements made for the replacement/follow-on to EVS PoC. The Contractor shall provide a transition team to assist the Government and the follow-on Contractor during the transition period.

The Contractor shall perform phase-out activities necessary for transition to follow-on services at the end of the EVS PoC Sustainment contract performance period. The Contractor shall include Phase-Out Transition activities within the Transition Plan that describe the methodology, processes, and phase-out activities.

The Contractor Phase-Out Transition Plan shall provide phase-out support that includes but not limited to the following steps:

a. Coordinating with contract phase-out activities
b. Updating, validating, and transferring of inventory and support documentation;
c. Participating in phase-out transition activities

The Contractor shall assist VA in the transition of EVS PoC services to the follow-on Contractor. The Contractor shall coordinate and transfer all EVS PoC management and technical data, such as site and desktop configurations, inventory, core and site(s) design diagrams and schematics. The Contractor shall comply with arrangements made for the replacement/follow-on to EVS PoC. The Contractor shall provide a transition team to assist the Government and any follow-on Contractor during the transition period.

Contractor shall address warranty transfer, maintenance as applicable for follow on entity to assume responsibility of contractor acquired government property/services. The Phase-Out Plan shall be delivered no later than 60 days prior to the end of the contract POP.

Deliverables:

B. Phase-Out Transition Plan

5.3 OPERATIONS, MAINTENANCE, ADMINISTRATION, PROVISIONING, AND REPAIR (OMAPR)

The Contractor shall operate, maintain, administer, provision, repair, and conduct end-to-end monitoring of the EVS PoC environment throughout the period of performance, while providing telecommunications services to the designated VA locations. This includes all related hardware, software, and licenses needed to provide a fully functional voice service. The Contractor shall receive, manage, and complete repair requests requiring EVS PoC specific support. Any repair or maintenance request shall be worked through trouble tickets and be trackable and auditable with detail such as type of repair requested, activities performed and by whom, resolution, and timestamps. The Contractor shall maintain the accuracy of EVS PoC OMAPR records. The Contractor shall utilize existing VA tools, listed in Addendum D, in performance of EVS PoC OMAPR functions. The Contractor shall update OMAPR templates and other documents as directed by VA.

5.3.1 OMPAR REPORTS

5.3.1.1 DAILY OPERATIONS REPORT

The Contractor shall develop and publish (e.g., email) an EVS PoC Daily Operations Summary Report. The EVS PoC Daily Operations Summary Report content will summarize the service degradations and disruptions, and change requests/orders that occurred during the prior 24 hour reporting period. A draft EVS PoC Daily Operations Summary Report template shall be delivered 45 days after contract award. The final EVS PoC Daily Operations Summary Report template shall be delivered 14 days after the Contractor has received comments from the VA. The first EVS PoC Daily Operations Summary Report shall be delivered within 7 days after the template has been finalized. The Contractor shall deliver an updated report on a daily basis thereafter. VA may request changes to the content, format, and time of delivery of the report. Such minor changes are anticipated to occur approximately daily for the first week after delivery starts and not more than once a month thereafter.

5.3.1.2 WEEKLY OPERATIONS REPORT

The Contractor shall develop and publish an EVS PoC Weekly Operations Report. The EVS PoC Weekly Operations Report content will focus on the quantity and performance of EVS PoC services, configuration items, and operations activities. A draft EVS PoC Weekly Operations Report template shall be delivered 60 days after contract award. The final EVS PoC Weekly Operations Report template shall be delivered 14 days after the Contractor has received comments from the VA. The first EVS PoC Weekly Operations Report shall be delivered within 14 days after the template has been finalized. The Contractor shall deliver an updated report on a weekly basis thereafter. VA may request changes to the content, format, and day of delivery of the report. Such minor changes are anticipated to occur approximately weekly during the first two months after delivery starts and not more than once a quarter thereafter.

5.3.1.3 MONTHLY OPERATIONS REPORT

The Contractor shall develop and publish an EVS PoC Monthly Operations Report. The EVS PoC Monthly Operations Report content will focus on performance and efficiency of, and risks to EVS PoC services, and operations activities. A draft EVS PoC Monthly Operations Report template shall be delivered 75 days after contract award. The final EVS PoC Monthly Operations Report template shall be delivered 14 days after the Contractor has received comments from the VA. The first EVS PoC Monthly Operations Report shall be delivered within 30 days after the template has been finalized. The Contractor shall deliver the report on or before the 10th day of each month. VA may request changes to the content, format, or day of delivery of the report. Such minor changes are anticipated to occur approximately three times during the first quarter after delivery starts and not more than twice a year thereafter.

5.3.1.4 DASHBOARD

The Contractor shall develop and maintain an online EVS PoC Dashboard on VA's Intranet. The dashboard will provide graphical performance data at various VA organizational levels, and EVS PoC service segments. A draft EVS PoC Dashboard shall be delivered 90 days after contract award. The first EVS PoC Dashboard shall be published 180 days after contract award.

Deliverables:

A. EVS PoC Daily Operations Summary Report Template
B. EVS PoC Daily Operations Summary Report
C. EVS PoC Weekly Operations Report Template
D. EVS PoC Weekly Operations Report
E. EVS PoC Monthly Operations Report Template
F. EVS PoC Monthly Operations Report
G. EVS PoC Dashboard

5.3.2 SERVICE DESK & TECHNICAL SUPPORT

5.3.2.1 EVS PoC MULTI-TIER SUPPORT APPROACH

EVS PoC utilizes a multi-tier support structure. A high-level description of the functions provided by Tiers 0 through 3 is provided in following table:

Table 5.1 - Technical Support Tier Descriptions

Technical Support Tier	High-Level Description
Tier 0	The first level of service provider functions, which is to collect and/or confirm customer and service request information in order to create, prioritize, and assign tickets to appropriate service providers for resolution.

Tier 1	The second level of service provider functions, which include problem screening, definition, and resolution. Service requests that cannot be resolved at this level in a set period of time are elevated to appropriate service providers at the Tier 2 level.
Tier 2	The third level of service provider functions, which consist primarily of problem identification, diagnosis, and resolution. Service requests that cannot be resolved at the Tier 2 level are typically referred to the Tier 3 for resolution.
Tier 3	The highest level of support. Problem resolution and defect management functions performed at this level usually require specialized resolution and possibly involvement and coordination with the manufacturer.

The roles and responsibilities of each support tier are further described in the sections below, and in the EVS PoC Technical Support Tier Matrix, attached.

5.3.2.1.1 VA NATIONAL SERVICE DESK (NSD)

NSD is provided by VA and is the designated service desk for EVS PoC, providing Tier 0 support services to end users. NSD operates 7 days a week, 24 hours a day. NSD opens user tickets, and provides first contact resolution (FCR) services for basic EVS PoC user requests; e.g., telephone set user manual or training.

5.3.2.1.2 VA LOCAL TELECOM TECHNICAL SUPPORT TEAMS

Local telecom technical support teams are provided by VA. The local telecom support teams provide Tier 1 technical support services to EVS PoC users. VA telecom technical support teams normally operate 5 days a week, 8 hours a day; excluding holidays.

5.3.2.1.3 VA SERVICE LINE TECHNICAL SUPPORT TEAMS

Service Line staff are provided by VA. Service Line staff provide Tier 1 services for ACD and IVR capabilities at the local and distribution layers of the EVS PoC architecture. Service Line staff provide Tier 2 and Tier 3 services for the distribution and local architecture layers of EVS PoC. Service Line staff normally operate 5 days a week, 8 hours a day; excluding holidays.

5.3.2.1.4 EVS HELPDESK

The Contractor shall provide all staff for the EVS Helpdesk. The Contractor shall staff the EVS Helpdesk 24 hours a day, 7 days a week. The Contractor's EVS Helpdesk staff shall be located at and shall conduct all EVS Helpdesk functions from one (1) VA location in TBD (tentatively Falling Waters, VA); and shall use GFE.

The Contractor personnel shall monitor all EVS infrastructure at the core, distribution, and local facility level; including but not limited to all items listed in Addendum D, D.1.2 - System Performance, Monitoring, and Reporting.

5.3.2.1.4.1 EVS HELPDESK TIER 1 THROUGH TIER 3 SERVICES

The Contractor shall provide Tier1 through Tier 3 services from the EVS Helpdesk location as described below. All EVS Helpdesk functions shall be provided at VA premise. Off premise / remote access / telework is not permitted.

- The Contractor shall remotely provide Tier 1 through Tier 3 services for EVS Core hardware and software.
- The Contractor shall remotely provide backup to Service Line staff providing Tier 2 and Tier 3 services for EVS distribution layer systems.
- The Contractor shall remotely provide backup to Service Line staff providing Tier 2 and Tier 3 services for EVS local layer systems.

Tier 1 through Tier 3 services provided by the Contractor shall include, but are not limited to the functions listed in the following table:

Table 5.2 - Tier Support Functions

TIER	FUNCTIONS
1	• Opens tickets for incidents or problems identified by EVS Helpdesk staff • Triages issues • Performs scripted diagnostics and resolution • Able to resolve basic or common problems
2	• Assesses nature of issue, reproducibility, and prior remediation steps attempted • Performs unscripted diagnostics and resolution • Performs detailed inspection or debugging of OS, configurations, applications and hardware • Repairs/replaces failed hardware or software components • Corrects configurations • Implements changes
3	• Diagnoses and resolves acute or chronic issues • Identifies systemic manufacturing defects in hardware and software • Identifies defects in or deviations from configuration and architecture standards • Manages defect resolution with defect owner; e.g., manufacturer, architect, or developer • Manages external support relationships and contracts • Receives and evaluates manufacturer tech bulletins • Receives, assesses, and tests patches with bug or vulnerability fixes • Plans changes • Escalates unresolved issues to Tier 4 (manufacturer, architect, or developer)

5.3.2.1.4.2 EVS PoC HELPDESK STAFF TECHNICAL CERTIFICATION REQUIREMENTS

EVS PoC currently utilizes technologies from Cisco, Microsoft, and VMware. The Contractor's staff shall hold current manufacturer certifications, specified below, on the hardware and software that currently constitute EVS PoC. Additionally, the Contractor shall provide staff with equivalent certification levels for any new technologies introduced into EVS PoC by the Contractor.

- Contractor personnel performing Tier 1 functions on Cisco technologies shall have a current Cisco Certified Network Associate Voice (CCNA Voice) certification or higher.
- Contractor personnel performing Tier 2 functions on Cisco technologies shall have a current Cisco Certified Network Professional Voice (CCNP Voice) certification or higher.
- Contractor personnel performing Tier 3 functions on Cisco technologies shall have a current Cisco Certified Internet Engineer Collaboration (CCIE Collaboration) certification or higher.

- Contractor personnel performing Tier 1 functions on Microsoft technologies shall have a current Microsoft Technology Associate (MTA) certification or higher.
- Contractor personnel performing Tier 2 functions on Microsoft technologies shall have a current Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 certification or higher.
- Contractor personnel performing Tier 3 functions on Microsoft technologies shall have a current Microsoft Certified Solutions Expert (MCSE) Server Infrastructure certification or higher.

- Contractor personnel performing Tier 1 functions on VMware technologies shall have a current VMware Certified Associate - Data Center Virtualization (VCA-DCV) or higher.
- Contractor personnel performing Tier 2 functions on VMware technologies shall have a current VMware Certified Professional 5 - Data Center Virtualization (VCP5-DCV) or higher.
- Contractor personnel performing Tier 3 functions on VMware technologies shall have a current VMware Certified Advanced Professional 5 - Data Center Administration (VCAP5-DCA) or higher.

5.3.2.1.4.3 EVS HELPDESK BUSINESS CONTINUITY PLAN

The Contractor shall develop and maintain an EVS Helpdesk Business Continuity Plan. The Business Continuity Plan (BCP) shall focus on sustaining the EVS Helpdesk's mission/business processes during and after a disruption. Examples of disruptions include, but are not limited to, loss of access to ticket system, loss of access to monitoring system, loss of network connectivity, loss of access to the building or facilities. The Contractor shall coordinate with information system owners, of information systems (IS) used by the EVS Helpdesk, to ensure that the BCP expectations and IS capabilities are matched. A draft BCP template shall be delivered 90 days after contract award. A final BCP template shall be delivered 30 days after the Contractor has received comments from the VA. A draft BCP document shall be delivered 60 days after the template has been finalized. A final BCP document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.2.1.5 *TIER 4* MANUFACTURER SUPPORT

While the manufacturer will provide Tier 4 and above technical support for EVS PoC components, the Contractor shall be responsible for escalating issues to the

manufacturer or developer, opening Tier 4 trouble ticket cases, and managing each case to ensure VA is receiving the appropriate response to meet business needs.

The Contractor shall develop and maintain an EVS PoC Site Access Procedures Document. The document shall include information for the EVS Helpdesk to arrange for the delivery of replacement parts or arrival of manufacturer technicians at each EVS PoC location. Examples of the information to be contained in the document include but are not limited to addresses, normal access hours, procedures for delivering packages during or after business hours, procedures for a manufacturer technician to access the facility during or business after hours, and points of contact to arrange or schedule access. A draft procedures template shall be delivered 60 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA.. A draft procedures document shall be delivered 30 days after the template has been finalized.. An initial procedures document shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall audit and update the procedures document annually.

5.3.2.1.6 MANUFACTURER SUPPORT CONTRACTS

The Contractor shall maintain all manufacturer EVS PoC Core configuration item e.g., hardware and software that do not have an end-of-support status from the manufacturer, under a manufacturer warranty support contract per the requirements listed in tables D.1 and D.2 in Addendum D in Section D.1.1.1. All EVS PoC configuration items located at an EVS PoC Core location are classified as EVS PoC Core configuration items. The Contractor shall purchase initial manufacturer warranty support, per the tables, for one (1) year for any new EVS PoC configuration items purchased by the Contractor. The Contractor shall manage the timely transfer of EVS PoC Core configuration items from initial manufacturer support contracts to the appropriate VA national manufacturer support contract; such that EVS PoC Core configuration items are always covered under manufacturer support per the D1. And D2 tables found in Addendum D Section D.1.1.1. If a VA national support contract is not available for the configuration item, the Contractor shall purchase continued support from the manufacturer per the D.1 and D.2 tables.. The Contractor shall update manufacturer support contract information as needed whenever changes (e.g., relocation or replacement) to configuration items (CIs) occur. The Contractor shall transfer ownership of EVS PoC manufacturer support contracts as directed by VA. The Contractor shall recommend changes to or renewal of maintenance support and/or spare parts for EVS PoC components within a time frame suitable to avoid EVS PoC missing customer SLA targets. Manufacturer or 3rd party support contracts and personnel must comply with VA personnel security requirements.

The Contractor shall track manufacturer support contracts by CI, in an EVS PoC Manufacturer Support Contract List. The list also shall contain all EVS PoC CIs without a manufacturer support contract. A draft list template shall be delivered 60 days after contract award. A final list template shall be delivered 30 days after the Contractor has received comments from the VA. A draft list shall be delivered 30 days after the template has been finalized. The initial list shall be delivered 300 days after the Contractor has received comments from the VA.

The Contractor shall provide an EVS PoC Manufacturer Support Contract Quarterly Report. The report shall include a list of all EVS PoC CIs without a manufacturer support contract as specified in the D.1 and D.2 tables, or any CI with a manufacturer support contract expiring within the next 18 months. A remediation plan or recommendation shall be provided for each CI listed in the report. A draft report template shall be delivered 100 days after contract award. A final report template shall be delivered 35 days after the Contractor has received comments from the VA. A draft report shall be delivered 35 days after the template has been finalized. The initial report shall be delivered 30 days after the Contractor has received comments from the VA. Subsequent reports shall be delivered by the 10th day of each calendar quarter.

The Contractor shall provide an annual EVS PoC Manufacturer Support Contract Audit Report. As part of the annual audit, the Contractor shall verify that each EVS PoC CI has the appropriate level of manufacturer support, and that manufacturer support is not being paid for unnecessarily; e.g., for disposed CIs. The Contractor shall reconcile any variances identified. A draft report template shall be delivered 100 days after contract award. A final report template shall be delivered 35 days after the Contractor has received comments from the VA. A draft report shall be delivered 35 days after the template has been finalized. The initial report shall be delivered 30 days after the Contractor has received comments from the VA. Subsequent reports shall be delivered by March 31st of each year.

5.3.2.1.7 REMOTE HANDS SUPPORT

Local technical support personnel will provide remote hands services under the direction of the Contractor.

5.3.2.2 REQUEST FULFILMENT

Request fulfilment documents, manages, and resolves customer requests for service throughout the service request lifecycle. Examples of service requests include moving, adding, changing, or disconnecting service; frequently referred to as MACD (Move, Add, Change, Disconnect). A customer request also may be for information regarding service.

The Contractor shall provision customer service requests on EVS PoC Core systems. EVS PoC Core service requests are limited to voicemail services. VA local telecom staff and Service Line staff are responsible for provisioning services on non-Core systems. The Contractor shall process service requests at the EVS Helpdesk. Any request fulfilment involving the Contractor shall be trackable and auditable in the National Service Desk ticketing system with details such as type of request, activities performed and by whom, and timestamps. The expected volume of EVS PoC Core service requests at time of contract award is provided in the following table. EVS PoC Core service request volume is anticipated to decrease to zero as voicemail is migrated out of the EVS PoC Core.

Table 5.3 – EVS PoC Core Service Request Volume

Busy Hour Average	
Business Day Average	

Non-Business Day Average	

The Contractor shall complete 95% of individual service requests within 30 minutes for voicemail password resets and 1 business day for other requests. The Contractor shall complete 100% of individual service requests within 60 minutes for voicemail password resets and 3 business days for other requests. The Contractor shall process bulk service requests; e.g., a workgroup move; within 10 business days. The Contractor shall accommodate requests that specify a specific date and/or time for a MACD; including after business hours. The Contractor shall assist site support personnel with completing password resets for other EVS PoC services; e.g., contact center agent; after business hours.

The Contractor shall update and publish EVS PoC Request Fulfillment Procedures. The procedures shall describe the steps for performing any manual request fulfillment activities normally executed by the Contractor. The procedures shall include the expected response, if any, from a system after each step or command is executed. . A draft procedures template shall be delivered 60 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.2.3 EVENT MANAGEMENT

Event Management monitors services, configuration items, and processes; and manages events throughout their lifecycle. Event Management includes detection, collection, logging, correlation, validation, categorization, and prioritization of infrastructure, service, business, and security events; and filters out events that do not require a response. Event Management focuses on root conditions that indicate or could lead to potential faults or Service Level exceptions. The root conditions are analyzed and appropriate action(s), if required, are taken.

The Contractor shall perform Event Management for all EVS PoC services, configuration items (CIs), and processes utilizing Contractor managed; e.g., ScieneLogic; and VA managed systems, applications, and tools; e.g., SolarWinds. A complete list of monitoring tools used by EVS PoC is provided in Addendum H, Section XX. The Contractor shall ensure that all EVS PoC services, configuration items, and processes are monitored through proactive, active, passive, or reactive means. Proactive monitoring looks for patterns of events to predict possible future failures. Active monitoring utilizes automated regular checks to discover the current status. Passive monitoring utilizes an alert or notification, from the service, configuration item, or process, to discover the current status. Reactive monitoring takes place in response to an event; e.g., submitting a batch job when the previous job completes. The Contractor shall; to the extent possible with in place systems, applications, and tools; convert reactive monitoring mechanisms to proactive, active, or passive mechanisms. The Contractor is responsible for configuring and managing the ScienceLogic software and hardware used to monitor EVS PoC.The Contractor shall utilize ScienceLogic to maintain or improve mechanisms for generating meaningful EVS PoC events and

effective rules for their filtering and correlating. This may require coordinating with other VA organizations to set up, maintain, or improve EVS PoC event filtering in other monitoring applications e.g., SolarWinds. The mechanisms shall filter out events which are merely informational and can be ignored; and to communicate, via alerts presented in network management systems (NMS), any event that indicates an abnormal condition, a service degradation, or service disruption. The Contractor shall interpret the meaning of an event and select a suitable response if required. The Contractor shall check if events have been handled appropriately and may be closed. The Contractor shall analyze event logs, monthly, in order to identify trends or patterns which suggest corrective action must be taken.

The Contractor shall; to the extent possible with in place systems, applications, and tools; have events, which result in a Priority 1 or Priority 2 incident (As described in Addendum D Table D.1 “NSD Incident Priority Matrix”), generate an alert that is presented to the Contractor’s EVS Helpdesk staff within 10 minutes of the event occurring. This requirement does not apply when the event is prevented from being presented to the Contractor’s EVS Helpdesk staff by a limitation or breakdown in government managed hardware, software, processes, procedures, or partners.

The Contractor shall maintain an EVS PoC Event Management Library of Rules. The Contractor shall develop new or update existing EVS PoC Event Management Rules to improve event management; to support new EVS PoC hardware or software , or to support new EVS PoC services that come on line. The library shall contain a list of each EVS PoC Event Management rule in use in EVS PoC managed systems. Each rule in the library shall have a unique identifier, name, and description. Each rule also shall include why, where, when, and how it is used; and identify any interdependencies with other rules. The Contractor shall include source code, if any, for rules in the library. The Contractor shall update the library within 10 days of any changes to EVS PoC Event Management rules.

The Contractor shall develop and publish EVS PoC Event Management Procedures. The procedures shall describe the steps for performing any manual activities used for EVS PoC Event Management. The procedures shall include the expected response, if any, from a system after each step or command is executed. A draft procedures template shall be delivered 60 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall provide an EVS PoC Event Management Monthly Audit Report. The report shall include any EVS PoC event trends or patterns which suggest corrective action must be taken, and shall include any events that must be reclassified or event handling changed. For each item listed, the report shall include a recommended remediation action and status. The report shall carry over from prior reports any unresolved/open items. A draft report template shall be delivered 30 days after contract award. A final report template shall be delivered 15 days after the Contractor has received comments from the VA. The initial report shall be delivered 30 days after the

template has been finalized. Subsequent reports shall be delivered the 10th of each month.

5.3.2.4 EVENT HANDLING

5.3.2.4.1 NETWORK MANAGEMENT SYSTEM ALERTS

The Contractor shall initiate response to 95% of EVS PoC system alerts in the network management system (NMS) within 5 minutes; measured on a monthly basis. The Contractor shall initiate response to 100% of EVS PoC alerts in the network management system (NMS) within 60 minutes, measured on a monthly basis. Response time is measured from the time the alert was presented to the EVS Helpdesk in the NMS to the time the alert was acknowledged by the Contractor. The expected volume of EVS PoC events at time of contract award is provided in the following table. Event volume is anticipated to remain flat during the base year. Event volume during option years may increase if additional VA locations are added to EVS PoC. Spikes in event volume may occur during scheduled maintenance of EVS PoC systems or other systems to which EVS PoC is connected.

Table 5.4 – EVS Helpdesk NMS Event Volume

Busy Hour Average	
Business Day Average	
Non-Business Day Average	

5.3.2.4.2 TELEPHONE CALLS

The Contractor shall answer EVS Helpdesk telephone calls within 18 seconds 95% of the time; measured on a monthly basis. The Contractor shall answer telephone calls within 42 seconds 100% of the time; measured on a monthly basis. Inbound user calls are handled by NSD, not the Contractor (EVS Helpdesk) Examples of inbound calls to the EVS Helpdesk include EVS PoC support staff from Field Operations (site, VISN, and Service Line), NSD, manufacturer support (Cisco), data center support (Enterprise Operations), and LECs. The expected volume of calls to the EVS Helpdesk at time of contract award is provided in the following table. Call volume is anticipated to remain flat during the base year. Call volume during option years may increase if additional VA locations are added to EVS PoC. Spikes in call volume may occur during scheduled maintenance of EVS PoC systems or other systems to which EVS PoC is connected.

Table 5.5 – EVS Helpdesk Telephone Call Volume

Busy Hour Average	
Business Day Average	
Non-Business Day Average	

5.3.2.4.3 EMAILS

The Contractor shall respond to 95% of email notifications of EVS PoC events within 30 minutes; measured on a monthly basis. The Contractor shall respond to 100% of email notifications of EVS PoC events within 60 minutes; measured on a monthly basis.

Response time is measured from the time stamp of the inbound email to the time stamp of the outbound email. The expected volume of emails to the EVS Helpdesk at time of contract award is provided in the following table. Email volume is anticipated to remain flat during the base year. Email volume during option years may increase if additional VA locations are added to EVS PoC. Spikes in email volume may occur during scheduled maintenance of EVS PoC systems or other systems to which EVS PoC is connected.

Table 5.6 – EVS Helpdesk Email Volume

Busy Hour Average	
Business Day Average	
Non-Business Day Average	

5.3.2.5 INCIDENT MANAGEMENT

Incident Management concentrates on restoring unexpectedly degraded or disrupted normal service operation to users as quickly as possible, in order to minimize the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Incident Management includes coordination of appropriate resources and communication of incident related information for situational awareness as quickly as possible. The Contractor shall perform Incident Management for EVS PoC.

The Contractor shall manage the lifecycle of EVS PoC incidents assigned to or owned by the EVS Helpdesk. This includes identification, logging, categorization, prioritization, diagnosis, restoration, recovery, and repair. This includes requesting and coordinating VA and non-VA resources that are necessary to restore normal EVS PoC service operation as quickly as possible.

The Contractor shall open an incident ticket is for each EVS PoC incident the Contractor detects. The Contractor shall prioritize incidents according to the VA National Service Desk (NSD) Incident Prioritization Matrix depicted in Addendum D1.1. The Contractor shall perform management escalations and technical escalations as needed to acquire and bring to bear VA and non-VA resources necessary to restore EVS PoC services within the SLAs specified in Addendum D Section D 1.0.

The Contractor shall update and/or develop, and publish EVS PoC Incident Management Procedures. Current EVS PoC incident management procedure documents are listed in Addendum G and attached to this PWS. The procedures or runbooks shall describe the steps for performing any manual activities used for EVS PoC Incident Management. The procedures shall include the expected response, if any, from a system after each step or command is executed. A draft procedures document shall be delivered 120 days after contract award. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop and publish EVS PoC Escalation and Notification Procedures. The document shall describe the time intervals, contacts, methods, and steps for performing any activities used for EVS PoC Incident notifications or escalations. The escalation and notification procedures shall comply with EVS PoC

Program/Project and NSD requirements. A draft procedures template shall be delivered 60 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop and publish an EVS PoC Escalation and Notification Contacts list. The document shall list internal and external administrative (e.g., NSD), managerial (e.g., EVS PoC Program), and technical (e.g., EVS PoC OEM contact information used to report and escalate EVS PoC incidents. A draft list template shall be delivered 60 days after contract award. A final list template shall be delivered 30 days after the Contractor has received comments from the VA. A draft list shall be delivered 30 days after the template has been finalized. The initial list shall be delivered 30 calendar days after the Contractor has received comments from the VA. The Contractor shall verify/audit the list annually each November, and publish an updated list by December 15th each year.

The Contractor shall develop and publish an EVS PoC Supplier Service Level Agreements document. The document shall provide a consolidated list of all VA and non-VA organizations that supply services; e.g., LAN, WAN Service Desk; to EVS PoC. The document shall include the service performance parameters each supplier has agreed to provide to EVS PoC. A draft document template shall be delivered 90 days after contract award. A final document template shall be delivered 30 days after the Contractor has received comments from the VA. A draft document shall be delivered 30 days after the template has been finalized. The initial document shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall verify/audit the document annually each November, and publish an updated document by December 15th each year.

5.3.2.6 INCIDENT HANDLING

The Contractor shall respond to 95% of priority 1 and 2 incidents affecting any EVS PoC service within 5 minutes, measured on a monthly basis. The Contractor shall respond to 100% of priority 1 and 2 incidents affecting any EVS PoC service within 10 minutes, measured on a monthly basis. The Contractor shall respond to 95% of priority 3 EVS PoC incidents involving EVS PoC Core components within 1 hour, measured on a monthly basis. The Contractor shall respond to 100% of priority 3 EVS PoC incidents involving EVS PoC Core components within 2 hours, measured on a monthly basis. The Contractor shall respond to 95% of priority 4 EVS PoC incidents involving EVS PoC Core components within 1 business day, measured on a monthly basis. The Contractor shall respond to 100% of priority 4 EVS PoC incidents involving EVS PoC Core components within 2 business days, measured on a monthly basis. Response time is measured from the time stamp of the initial notification to the time stamp of when the incident ticket was created. The expected volume of EVS PoC incidents at time of contract award is provided in the following table. Incident volume is anticipated to remain flat during the base year. Incident volume during option years may increase if additional VA locations are added to EVS PoC. Spikes in incident volume may occur

following scheduled maintenance of EVS PoC systems or other systems to which EVS PoC is connected.

Table 5.7 – EVS PoC Incident Volume

	PRIORITY 1 & 2	PRIORITY 3 EVS PoC Core Only	PRIORITY 4 EVS PoC Core Only
Busy Hour Average			
Business Day Average			
Non-Business Day Average			

The Contractor shall resolve 95% of EVS PoC incidents, caused by EVS PoC Core hardware or software, within the SLAs listed in the table below, measured on a monthly basis. The SLAs do not apply to EVS PoC incidents caused by EVS PoC components in the EVS PoC local/access or distribution architecture layers. The SLAs do not apply to EVS PoC incidents caused by non-EVS PoC hardware, software, infrastructure, or services; e.g., LAN, WAN, PSTN, Power, HVAC. The resolution time is measured from the time the ticket is first assigned to the Contractor to the time EVS PoC service is restored to normal operation.

For EVS PoC incidents caused by non-EVS PoC hardware, software, infrastructure, or services; the Contractor shall make every effort; e.g., coordination and escalation with responsible organizations; to resolve the incident within the time-to-resolve periods specified in the table below. For EVS PoC incidents caused by EVS PoC local/access or distribution components, the Contractor shall assist with resolution activities at the request of Facility, VISN, or Service Line telecom support staff.

Table 5.8 - Incident Resolution SLAs

INCIDENT RESOLUTION SLA	
INCIDENT TICKET PRIORITY	**TIME TO RESOLVE**
1	2 Hours
2	4 Hours
3	8 Hours
4	5 Days

5.3.2.7 PROBLEM MANAGEMENT

Problem Management manages the lifecycle of all problems, where a problem is defined as the unknown cause of one or more incidents. The lifecycle includes proactive

activities to detect, and prevent or minimize the impact of future problems/incidents by diagnosing the root cause of incidents, determining the resolution of those incidents, the development of a known error sub-process to allow quicker diagnosis and resolution if future incidents do occur, and ensuring that the resolution is implemented through appropriate change control procedures. The Contractor shall perform Problem Management for EVS PoC.

The Contractor shall analyze incident records and other EVS PoC data; e.g., events; to proactively identify problems. The Contractor shall participate in the NSD root cause analysis and after action reporting processes for all Priority 1 and 2 EVS PoC incidents. The Contractor shall perform Problem Management for other EVS PoC issues as directed by VA. The Contractor shall log, categorize, and prioritize EVS PoC problems. The Contractor shall ensure a problem ticket is opened for each EVS PoC problem. For EVS PoC problems assigned/owned by the EVS Helpdesk, the Contractor shall investigate and diagnose the problem, create a workaround or solution, resolve the problem, and create a known error record. The Contractor shall request and coordinate VA and non-VA resources that are necessary to diagnose and resolve problems. The Contractor shall track the status of EVS PoC problems and perform management escalations for any problems that have exceeded or are expected to exceed the planned resolution date.

The Contractor shall develop and maintain records in the EVS PoC Known-Error Database (KEDB); a SharePoint repository. The Contractor shall create, review, edit, and publish EVS PoC known errors. The Contractor shall audit known-error records in the KEDB annually. The Contractor shall republish, update, or rescind EVS PoC known errors in the KEDB as needed. The Contractor shall modify or move the EVS PoC KEDB in SharePoint as needed or directed by VA.

The Contractor shall update and publish EVS PoC Problem Management Procedures. The procedures shall describe the steps for performing any manual activities used for EVS PoC Problem Management. The procedures shall include the expected response, if any, from a system after each step or command is executed. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA. The expected volume of EVS PoC problems at time of contract award is provided in the following table. Problem volume is anticipated to remain flat during the base year. Problem volume during option years may increase if additional hardware or software is added to EVS PoC. Spikes in problem volume may occur following scheduled maintenance of EVS PoC systems or other systems to which EVS PoC is connected.

Table 5.9 – EVS PoC Problem Volume

Weekly Average	
Problems Open – Pending Analysis	
Problems Open – Analysis Complete - Pending Resolution	

Deliverables:

A. EVS PoC Site Access Procedures Template
B. EVS PoC Site Access Procedures
C. EVS PoC Enterprise Helpdesk Business Continuity Plan Template
D. EVS PoC Enterprise Helpdesk Business Continuity Plan
E. EVS PoC Manufacturer Support Contract List Template
F. EVS PoC Manufacturer Support Contract List
G. EVS PoC Manufacturer Support Contract Quarterly Report Template
H. EVS PoC Manufacturer Support Contract Quarterly Report
I. EVS PoC Manufacturer Support Contract Audit Report Template
J. EVS PoC Manufacturer Support Contract Audit Report
K. EVS PoC Request Fulfillment Procedures Template
L. EVS PoC Request Fulfillment Procedures
M. EVS PoC Event Management Procedures Template
N. EVS PoC Event Management Procedures
O. EVS PoC Event Management Monthly Audit Report Template
P. EVS PoC Event Management Monthly Audit Report
Q. EVS PoC Incident Management Procedures
R. EVS PoC Incident Escalation and Notification Procedures Template
S. EVS PoC Incident Escalation and Notification Procedures
T. EVS PoC Incident Escalation and Notification Contacts Template
U. EVS PoC Incident Escalation and Notification Contacts
V. EVS PoC Supplier Service Level Agreements Template
W. EVS PoC Supplier Service Level Agreements
X. EVS PoC Problem Management Procedures Template
Y. EVS PoC Problem Management Procedures

5.3.3 EVS PoC ADMINISTRATION

Administration of EVS PoC includes managing the hardware, operating systems, applications, storage, and connectivity used to provide EVS PoC services.

5.3.3.1 SYSTEM ADMINISTRATION

System Administration involves the installation and maintenance of one or more computer systems and associated peripherals, internal hardware components, the operating system, virtual machines, and associated utility programs. System Administration ensures machines are maintained at an established baseline and updated with the latest security patches, upgrades, and encryption. System Administration releases hardware and operating system changes into the environment.

The Contractor shall develop, schedule, and perform system administration tasks for EVS PoC Core systems. The Contractor shall develop backup schedules, monitor operations of system hardware and software, and troubleshoot the system when a problem occurs. In addition, the Contractor shall tune the system to resolve or avoid performance issues.

The Contractor shall configure and install software, scripts and parameter settings. The Contractor shall create and administer backup schedules and media. The Contractor shall create infrastructure change orders/requests for scheduled system outages/preventative maintenance. The Contractor shall implement, repair, and upgrade system hardware and software. The Contractor shall monitor and maintain system logs and records. The Contractor shall monitor system resources, perform file transfers, and schedule production jobs.

The Contractor shall monitor EVS PoC systems for security, performance, fault, and configuration issues. The Contractor shall identify negative trends and repetitive issues, and notify VA. The Contractor shall optimize system performance, and shall implement changes to prevent or remediate system performance issues.

The Contractor shall monitor OEM tech bulletins for system releases, bugs, vulnerabilities, fixes, patches, and end-of-life notices. OEM includes any free or licensed software embedded within EVS PoC systems. The Contractor also shall monitor United States Computer Emergency Readiness Team (US-CERT) and VA Network Security Operations Center (NSOC) bulletins for vulnerabilities in EVS PoC system hardware and software. The Contractor shall identify, recommend, and implement system upgrades or patches necessary to remediate vulnerabilities or bugs. The Contractor shall identify, recommend, and implement upgrades and patches for EVS PoC systems hardware and software with an OEM end-of-life notice, or forecasted to be deprecated per the One-VA Technical Reference Model (TRM).

The Contractor shall schedule and conduct system backups that meet EVS PoC information system contingency plan and disaster recovery plan targets; including, but not limited to, recovery time objectives and recovery point objectives. At a minimum, the Contractor shall perform system backups daily or real-time with real-time mirroring/shadowing. At a minimum, the Contractor shall perform system documentation backups annually. At a minimum, the Contractor shall test system backup information to verify media reliability and information integrity weekly. At a minimum, the Contractor shall test system documentation backup information to verify media reliability and information integrity quarterly. The Contractor shall perform system restoration activities, and shall request manufacturer support for system issues.

The Contractor shall develop and maintain an EVS PoC System Administration Task Schedule for all reoccurring system administration tasks that are mandatory or recommended by the manufacturer. The document shall specify the frequency of each task and include, as appropriate, when the task must be executed (e.g., time of day, day of week, or day of month). The document shall identify, for each task, if the task is automated or manual. Automated means “fully” automated to include the starting and stopping of the task. Manual means any task that, in whole or in part, requires a human to perform an action. A draft task schedule template shall be delivered 180 days after contract award. A final task schedule template shall be delivered 30 days after the Contractor has received comments from the VA. A draft task schedule shall be delivered 30 days after the template has been finalized. A final task schedule shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall log completion of all reoccurring system administration tasks. The Contractor shall develop and maintain an EVS PoC System Administration Task Log. The log shall include a list of all system administration tasks. For each manual task in the log, the Contractor shall record the date and time the task was completed, and the name of the person that completed the task. For each automated task in the log with an automated mechanism to report failed tasks, no log entry is required. For each automated task in the log without an automated mechanism to report failed tasks, the Contractor shall record the date and time the task was completed, and the name of the person that verified the task completed successfully. A draft log template shall be delivered 90 days after contract award. A final log template shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall annotate completion of tasks in the log per the EVS PoC System Administration Task Schedule.

The Contractor shall develop and maintain an EVS PoC System Administration Task Procedures document for all reoccurring system administration tasks that are manual. The procedures document shall include step-by-step procedures to execute each task. The procedures shall include the expected response, if any, from the system after each step or command is executed. The procedures shall be specific for each type and version of system hardware and software utilized in EVS PoC. The EVS PoC System Administration Task Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC System Administration Task Procedures document. A draft procedures template shall be delivered 210 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.3.2 APPLICATION ADMINISTRATION

Application Administration schedules application/service tasks, develops backup schedules, monitors operations of the application/services software, and troubleshoots the application/service when a problem occurs. In addition, Application Administration participates in tuning the application/service to resolve performance issues.

The Contractor shall perform Application Administration for EVS PoC applications. The Contractor shall monitor EVS PoC applications, services, and other associated software for security, performance, fault, and configuration issues. The Contractor shall identify negative trends and repetitive issues, and notify VA. The Contractor shall optimize application performance, and shall implement changes to prevent or remediate application performance issues. The Contractor shall include applicable Application Administration data in the EVS PoC weekly and monthly operations reports.

The Contractor shall monitor original equipment manufacturer (OEM) tech bulletins for software releases, bugs, vulnerabilities, fixes, patches, and end-of-life notices. OEM includes any free or licensed software embedded within EVS PoC applications; e.g. Java, or .NET. The Contractor also shall monitor US-CERT and VA NSOC bulletins for vulnerabilities in EVS PoC applications and related software. The Contractor shall identify, recommend, and upon VA approval implement application upgrades or patches

necessary to remediate vulnerabilities or bugs. The Contractor shall identify, recommend, and upon VA approval implement application upgrades and patches for EVS PoC applications and related software with an OEM end-of-life notice, or forecasted to be deprecated per the One-VA Technical Reference Model (TRM).

The Contractor shall schedule and conduct application and application documentation backups that meet EVS PoC information system contingency plan and disaster recovery plan targets; including, but not limited to, recovery time objectives and recovery point objectives. At a minimum, the Contractor shall perform application and application documentation backups annually. At a minimum, the Contractor shall test application and application documentation backup information to verify media reliability and information integrity quarterly. The Contractor shall perform application restoration activities, and shall request manufacturer support for application issues.

The Contractor shall develop and maintain an EVS PoC Application Administration Task Schedule for all reoccurring application administration tasks that are mandatory or recommended by the manufacturer. The document shall specify the frequency of each task and include, as appropriate, when the task must be executed (e.g., time of day, day of week, or day of month). The document shall identify, for each task, if the task is automated or manual. Automated means “fully” automated to include the starting and stopping of the task. Manual means any task that, in whole or in part, requires a human to perform an action. A draft task schedule template shall be delivered 60 days after contract award. A final task schedule template shall be delivered 30 days after the Contractor has received comments from the VA. A draft task schedule shall be delivered 30 days after the template has been finalized. A final task schedule shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall provide an updated document within 10 days of any changes to EVS PoC components; manufacturer recommendations or requirements that affect EVS PoC Application Administration task schedules.

The Contractor shall log completion of all reoccurring application administration tasks. The Contractor shall develop and maintain an EVS PoC Application Administration Task Log. The log shall include a list of all application administration tasks. For each manual task in the log, the Contractor shall record the date and time the task was completed, and the name of the person that completed the task. For each automated task in the log with an automated mechanism to report failed tasks, no log entry is required. For each automated task in the log without an automated mechanism to report failed tasks, the Contractor shall record the date and time the task was completed, and the name of the person that verified the task completed successfully. A draft log template shall be delivered 90 days after contract award. A final log template shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall annotate completion of tasks in the log per the EVS PoC Application Administration Task Schedule.

The Contractor shall develop and maintain an EVS PoC Application Administration Task Procedures document for all reoccurring application administration tasks that are manual. The procedures document shall include step-by-step procedures to execute each task. The procedures shall include the expected response, if any, from the application after each step or command is executed. The procedures shall be specific

for each type and version of application utilized in EVS PoC. The EVS PoC Application Administration Task Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Application Administration Task Procedures document. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.3.3 STORAGE MANAGEMENT

Storage Management describes the function and processes responsible for management of storage and maintenance of data through its lifecycle. This includes scheduling Storage Management tasks (e.g., deleting or archiving log files), monitoring operations and capacity of the storage systems, and troubleshooting storage systems when a problem occurs. In addition, Storage Management participates in tuning storage systems to resolve performance issues.

The Contractor shall perform Storage Management for EVS PoC Core systems. The Contractor shall provision (install, configure, and allocate) storage, track storage utilization, and assure adequate space to accommodate growth. The Contractor shall decommission storage media; e.g., when media fails and needs to be replaced, or when media is obsoleted and needs to be disposed. The Contractor shall monitor EVS PoC storage systems hardware and software for security, performance, fault, and configuration issues. The Contractor shall identify negative trends and repetitive issues, and notify VA. The Contractor shall optimize storage performance, and shall implement changes to prevent or remediate storage performance issues. The Contractor shall optimize use of online and offline storage.

The Contractor shall monitor OEM tech bulletins for hardware and software releases, bugs, vulnerabilities, fixes, patches, and end-of-life notices. OEM includes any free or licensed software embedded within EVS PoC storage systems. The Contractor also shall monitor U.S. CERT and VA NSOC bulletins for vulnerabilities in EVS PoC storage systems. The Contractor shall identify, recommend, and implement storage upgrades or patches necessary to remediate vulnerabilities or bugs. The Contractor shall identify, recommend, and implement storage upgrades and patches for EVS PoC storage systems with an OEM end-of-life notice, or forecasted to be deprecated per the One-VA Technical Reference Model (TRM).

The Contractor shall develop and maintain an EVS PoC Storage Management Task Schedule for all reoccurring storage management tasks that are mandatory or recommended by the manufacturer. The document shall specify the frequency of each task and include, as appropriate, when the task must be executed (e.g., time of day, day of week, or day of month). The document shall identify, for each task, if the task is automated or manual. Automated means “fully” automated to include the starting and stopping of the task. Manual means any task that, in whole or in part, requires a human to perform an action. A draft task schedule template shall be delivered 90 days after contract award. A final task schedule template shall be delivered 30 days after the

Contractor has received comments from the VA. A draft task schedule shall be delivered 30 days after the template has been finalized. A final task schedule shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall log completion of all reoccurring storage management tasks. The Contractor shall develop and maintain an EVS PoC Storage Management Task Log. The log shall include a list of all storage management tasks. For each manual task in the log, the Contractor shall record the date and time the task was completed, and the name of the person that completed the task. For each automated task in the log with an automated mechanism to report failed tasks, no log entry is required. For each automated task in the log without an automated mechanism to report failed tasks, the Contractor shall record the date and time the task was completed, and the name of the person that verified the task completed successfully. A draft log template shall be delivered 90 days after contract award. A final log template shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall annotate completion of tasks in the log per the EVS PoC Storage Management Task Schedule.

The Contractor shall develop and maintain an EVS PoC Storage Management Task Procedures document for all reoccurring storage management tasks that are manual. The procedures document shall include step-by-step procedures to execute each task. The procedures shall include the expected response, if any, from the storage system after each step or command is executed. The procedures shall be specific for each type and version of storage system utilized in EVS PoC. The EVS PoC Storage Management Task Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Storage Management Task Procedures document. A draft procedures template shall be delivered 120 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from VA.

5.3.3.4 EVS PoC CONNECTION AND INTEGRATION POINT ADMINISTRATION

Administration of EVS PoC connections and integration points (connections) monitors operations of the connections to EVS PoC (e.g., LAN connections, PSTN connections, SIP trunks, connection to other unified communications (UC) applications, connections to E-911, connections to nurse call, etc.), and troubleshoots connections when a problem occurs. This includes tuning connections to resolve performance issues

The Contractor shall administer EVS PoC connections and integration points. The Contractor shall monitor EVS PoC connectivity to supporting voice and data communications infrastructure for security, performance, fault, and configuration issues. The Contractor shall identify negative trends and repetitive issues, and notify VA. The Contractor shall optimize connectivity performance, and shall initiate and implement changes to prevent or remediate performance issues with connections.

The Contractor shall monitor OEM tech bulletins for EVS PoC connection and interface related releases, bugs, vulnerabilities, fixes, patches, and end-of-life notices. OEM includes any proprietary, free, or licensed software embedded within EVS PoC

connection components. The Contractor also shall monitor U.S. CERT and VA NSOC bulletins for vulnerabilities in EVS PoC connection components and related software. The Contractor shall identify, recommend, and implement connection upgrades or patches necessary to remediate vulnerabilities or bugs. The Contractor shall identify, recommend, and implement upgrades and patches for EVS PoC connectivity components and related software with an OEM end-of-life notice, or forecasted to be deprecated per the One-VA Technical Reference Model (TRM).

The Contractor shall develop and maintain an EVS PoC Connections and Integration Points List. The list shall contain all physical and virtual connectivity to EVS PoC. All relevant information for each connection shall be provided; e.g., circuit identifier, IP address, physical/virtual port, far-end system name/identifier, far-end system owner, far-end system point-of-contact and contact information. A draft list template shall be delivered 60 days after contract award. A final list template shall be delivered 30 days after the Contractor has received comments from the VA. A draft list shall be delivered 30 days after the template has been finalized. The initial list shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall audit the list annually.

Deliverables:

A. EVS PoC System Administration Task Schedule Template
B. EVS PoC System Administration Task Schedule
C. EVS PoC System Administration Task Log Template
D. EVS PoC System Administration Task Procedures Template
E. EVS PoC System Administration Task Procedures
F. EVS PoC Application Administration Task Schedule Template
G. EVS PoC Application Administration Task Schedule
H. EVS PoC Application Administration Task Procedures Template
I. EVS PoC Application Administration Task Procedures
J. EVS PoC Application Administration Task Log Template
K. EVS PoC Storage Management Task Schedule Template
L. EVS PoC Storage Management Task Schedule
M. EVS PoC Storage Management Task Log Template
N. EVS PoC Storage Management Task Procedures Template
O. EVS PoC Storage Management Task Procedures
P. EVS PoC Connections and Integration Points List Template
Q. EVS PoC Connections and Integration Points List

5.3.4 BUILD AND RELEASE MANAGEMENT

Build and Release Management are the processes used to prepare new software, hardware, and capabilities for deployment into the EVS PoC environment.

5.3.4.1 BUILD MANAGEMENT

Build Management assembles Configuration Items into Build Packages, controls baseline versioning and manages the working library during development, updates and reports status of Change Orders addressed by Builds, conducts review of tested Release Package, ensures implementation of the tested Release, ensures back out of

Release (if necessary), provides Incident and Problem reports to appropriate Incident and Problem Management, provides Release status to Release Management, and provides Gold Build to Configuration Management.

The Contractor shall perform Build Management for EVS PoC. The Contractor shall develop EVS PoC Build Packages; which include but are not limited to technical manuals, architecture specifications and diagrams, System Design Document, interface control documents, database application mapping, database support processes and procedures, System Engineering Design Review, installation guides, back-out plan and procedures, user guides, and Version Description Document. The Contractor shall ensure that EVS PoC Build Packages are compliant with the VA Continuous Readiness and Information Security Program (CRISP), VA Enterprise Architecture (EA), and VA Technical Reference Model (TRM) standards. The Contractor shall recommend updates to CRISP, VA EA, and VA TRM standards that are applicable to EVS PoC. The Contractor shall monitor CRISP, VA EA, and VA TRM standards for changes affecting EVS PoC. The Contractor shall update, release, and implement EVS PoC Build Packages as needed to stay compliant with CRISP, VA EA, and VA TRM. The Contractor shall archive builds, document outstanding defects and workarounds, establish final release configuration (Build Package), implement approved changes, record/update Configuration Items. A draft build package template shall be delivered 150 days after contract award. A final build package template shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop, update, and publish an EVS PoC Build Schedule. The schedule shall include all EVS PoC planned builds. A draft schedule template shall be delivered 120 days after contract award. A final schedule template shall be delivered 30 days after the Contractor has received comments from the VA. An initial schedule shall be delivered 60 days after the template has been finalized.

The Contractor shall develop and maintain an EVS PoC Build Management Procedures document. The procedures shall include step-by-step instructions to execute each Build Management activity. The procedures shall include the expected response, if any, from a system after each step or command is executed. The EVS PoC Build Management Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Build Management Task Procedures document. A draft procedures template shall be delivered 210 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.4.2 RELEASE MANAGEMENT

Release Management ensures the planned and controlled deployment of hardware and software (e.g., commercial off the shelf (COTS) and Contractor developed scripts) into the Production environment. Process activities include ensuring that testing and verification are complete, that assets are available for deployment, and that necessary Configuration Items (CIs) are included in the Build. Release Management also ensures

that necessary training is provided to users and support personnel and that information about the release and its status is communicated to Stakeholders. The Release Management process does not perform the testing or provide the training it ensures that appropriate touch points that have this responsibility have completed the needed actions before approving the release.

The Contractor shall perform Release Management for EVS PoC. The Contractor shall confirm completion of build testing prior to production migration. The Contractor shall track and provide status on EVS PoC releases. The Contractor shall provide supporting documentation for final implementation and sign-off. The Contractor shall plan release deployments. The Contractor shall ensure that only tested and approved releases are deployed. The Contractor shall ensure the backout of releases if necessary. The Contractor shall ensure users and support personnel are trained on new releases prior to release deployment.

The Contractor shall develop an EVS PoC Release Plan for each new EVS PoC release. The release plan shall include, but is not limited to, release item information (e.g., name, business description, technical scope, business justification), release schedule, release contact information (e.g., sponsor, release manager, project manager, configuration manager, change manager), groups or areas affected by the release (e.g., user group, facility, services, infrastructure, projects), change management information, configuration management information, and supporting documentation.

The Contractor shall conduct and complete an evaluation of each release within 7 days after the release is deployed. The Contractor shall create and submit an EVS PoC Release Evaluation Report within 14 days after a release is deployed.

Deliverables:

A. EVS PoC Release Plan(s)
B. EVS PoC Release Evaluation Report(s)
C. EVS PoC Build Package Template
D. EVS PoC Build Package(s)
E. EVS PoC Build Schedule Template
F. EVS PoC Build Schedule
G. EVS PoC Build Management Procedures Template
H. EVS PoC Build Management Procedures

5.3.5 CHANGE, CONFIGURATION AND ASSET MANAGEMENT

Change, Configuration, and Asset Management are the processes used to add, remove, or modify components and capabilities in the EVS PoC environment.

5.3.5.1 CHANGE MANAGEMENT

Change Management ensures that standardized, documented, and repeatable methods and procedures are used for efficient and prompt handling of all changes, in order to minimize the impact of change-related incidents upon service quality, and consequently to improve the day-to-day operations of the organization. The Change Management

process ensures that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented, and reviewed in a controlled manner. This is accomplished by engaging other processes and roles like Application, Database, and System Administration, Configuration Management, Build Management, and Release Management.

The Contractor shall perform Change Management for EVS PoC. The Contractor shall be responsible for changes to the EVS PoC Core architecture layer, and shall participate in changes to EVS PoC distribution and site architecture hardware and software. The Contractor shall initiate, develop/plan, coordinate, implement, and validate EVS PoC changes. The Contractor shall ensure that all EVS PoC changes are compliant with VA security and technical policies and standards e.g., Assessment and Authorization, TRM, and CRISP. The Contractor shall ensure that all EVS PoC changes are successful. The Contractor shall ensure that a minimum of 95% of EVS PoC changes are completed within the scheduled and approved change/maintenance window for each change.

The Contractor shall create and submit change requests and/or change orders for the addition, modification, or removal of anything that could have an effect on EVS PoC services. “Anything” includes but is not limited to architecture, processes, tools, metrics, documentation, EVS PoC services, or other configuration items. Each change request shall include the proposed date and time (start and end) of the change, a change description, configuration items that are affected by the change, projected impact to EVS PoC services and SLAs, change procedures, change success criteria and evaluation procedures, backout plan and procedures, and criteria for triggering a backout. The Contractor shall submit change requests to the appropriate Change Control Board(s) within VA. The Contractor shall submit change requests/orders in a timely manner to allow change reviewers and local, regional, and national change authorities to review and approve changes within their published time/schedule for reviewing/approving changes. The Contractor shall not make a change to EVS PoC without prior approval.

The Contractor shall conduct an EVS PoC Change Review meeting weekly. During the meeting, the Contractor shall review EVS PoC changes scheduled during the previous week, approved EVS PoC changes scheduled during the following week, EVS PoC changes pending approval, and EVS PoC changes that are ready to be submitted to the appropriate VA Change Control Board(s) for approval. Also during the meeting, the Contractor shall review change notifications from other VA systems that may impact EVS PoC. The Contractor shall participate in other VA change management meetings to disseminate, review, brief, and discuss planned EVS PoC changes. The Contractor shall review, analyze, and comment on changes to other systems that may impact EVS PoC. The Contractor shall develop an EVS PoC Change Review Meeting Agenda Template and an EVS PoC Change Review Meeting Minutes Template. A draft of each template shall be delivered 15 days after contract award. A final of each template shall be delivered 15 days after the Contractor has received comments from the VA. The Contractor shall publish an EVS PoC Change Review Agenda prior to each meeting. The Contractor shall publish an EVS PoC Change Review Minutes after each meeting.

The Contractor shall develop, update, and publish an EVS PoC Change Schedule. The schedule shall include all EVS PoC changes in any status; e.g., approved, pending approval, draft; that are scheduled or tentatively scheduled during the next seven (7) days. The schedule also shall list changes to other VA systems scheduled during the following week that may impact EVS PoC. A draft schedule template shall be delivered 15 days after contract award. A final schedule template shall be delivered 7 days after the Contractor has received comments from the VA. An initial schedule shall be delivered 10 days after the template has been finalized.

The Contractor shall develop and maintain an EVS PoC Change Management Procedures document. The procedures document shall include step-by-step procedures to execute each Change Management activity. The procedures shall include the expected response, if any, from an application after each step or command is executed. The EVS PoC Change Management Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Change Management Procedures document. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA. The expected volume of EVS PoC changes at time of contract award is provided in the following table. Change volume is anticipated to remain flat during the base year. Change volume during option years may increase if additional VA locations are added to EVS PoC. Spikes in change volume may occur when manufacturer patches are released for EVS PoC technologies.

Table 5.10 – EVS PoC Change Volume

Weekly Average	

5.3.5.2 SCHEDULED MAINTENANCE WINDOWS

The Contractor shall schedule maintenance in accordance with VA, OI&T, Regional, VISN, Facility, and EVS PoC change control policies. The degradation of service, time frame, and purpose of the maintenance shall be described and approved by the VA Project Manager via email. Because of the nature of medical facilities, it is critical that any scheduled maintenance be coordinated and managed in such a way that the facility retains voice service (defined as the ability to place and receive calls) at any point in time and shall be coordinated on a site-by-site basis to have minimal impact on Veteran services and patient care.

The Contractor shall develop and maintain an EVS PoC Maintenance Window List. The list shall contain the maintenance window parameters agreed to by the appropriate stakeholders at each EVS PoC location. Each location entry in the list shall include, but is not limited to, window start time, window end time, and day(s) of week. The list also shall include, for each location if applicable, any maintenance moratorium periods during particular day(s) of month, quarter, or year. A draft list template shall be delivered 30 days after contract award. A final list template shall be delivered 15 days after the

Contractor has received comments from the VA. A draft list shall be delivered 30 days after the template has been finalized. The initial list shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.5.3 CONFIGURATION MANAGEMENT

Configuration Management defines and controls the components of services and infrastructure (Configuration Items) and maintains accurate configuration records. (ITIL v3 calls this Service Asset Configuration Management (SACM).

The Contractor shall perform Configuration Management for EVS PoC. The Contractor shall be responsible for tracking EVS PoC configuration items in the EVS PoC Core. The Contractor shall identify EVS PoC Core configuration items that are added, changed, or removed. The Contractor shall ensure that a configuration management record is created and maintained for each EVS PoC Core configuration item (CI). The Contractor shall ensure that EVS PoC configuration records include details such as how the CI is configured and the relationship between CIs. Examples of EVS PoC CIs and CI data include but are not limited to hardware, software, versions, interconnections and interfaces, configurations, support and maintenance contracts, certificates, leases, release dates, expiration dates, end-of-sale dates, end-of-maintenance dates, end-of-support dates, and documentation. The Contractor shall ensure that EVS PoC Core configuration items are under configuration control. The Contractor shall ensure that any EVS PoC configuration changes, needed as a result of maintenance changes, are captured and properly recorded.

The Contractor shall develop and publish EVS PoC Configuration Management Procedures. The procedures shall include step-by-step procedures for maintaining accurate data for all EVS PoC Core CIs; including but not limited to activities such as collecting, maintaining, and retiring CIs and CI data. Where applicable, the procedures shall be specific for each type and version of CI. The procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Configuration Management Procedures document. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall coordinate CI updates with EVS PoC local and Regional VA operations and maintenance staff. The Contractor shall verify and audit EVS PoC Core configuration items annually, and shall provide an EVS PoC Configuration Management Audit Report annually. The report shall identify any CI variances discovered during the audit, provide a POA&M to prevent similar discrepancies in CI data in the future, and a POA&M to locate and reconcile any missing CIs. The report shall carry over from prior reports any unresolved/open items, and identify any continuing or repetitive issues. A draft report template shall be delivered 330 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from

the VA. The initial report shall be delivered March 15th of option year one (1). Subsequent reports shall be delivered March 15th each year thereafter.

The Contractor shall provide an EVS PoC Configuration Management Detail Report within three business days upon request from the VA. The report shall include configuration management detail in a sortable MS Excel spreadsheet(s). The report shall include details as defined by VA for each report request.

5.3.5.4 ASSET MANAGEMENT

Asset Management provides EVS PoC asset availability information and requisition status and ensures EVS PoC asset deployment in support of scheduled releases. EVS PoC assets include fixed assets such as servers, soft assets such as software and licenses, and service assets such as resource or capability from a service provider.

The Contractor shall coordinate asset management activities with the appropriate asset managers within VA to maintain accurate EVS PoC asset data. The Contractor shall coordinate and assist with EVS PoC asset inventories and audits as needed, or directed by VA.

The Contractor shall develop and publish EVS PoC Asset Management Procedures. The procedures shall describe the steps for maintaining accurate asset management data for all EVS PoC assets; including but not limited to asset activities such as acquisition, replacement, relocation, sparing, and disposal. A draft procedures template shall be delivered 150 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 90 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall assist other VA organization with EVS PoC asset audits as needed, or directed by VA. The Contractor shall conduct an EVS PoC Asset Audit annually, and shall provide an EVS PoC Asset Audit Report annually. The report shall identify any asset variances discovered during the audit, provide a POA&M to prevent similar discrepancies in asset data in the future, and a POA&M to locate and reconcile any missing EVS PoC assets. The report shall carry over from prior reports any unresolved/open items, and identify any continuing or repetitive issues. A draft report template shall be delivered 330 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from the VA. The initial report shall be delivered March 15th of option year one (1). Subsequent reports shall be delivered March 15th each year thereafter.

The Contractor shall provide an EVS PoC Asset Management Detail Report within three business days upon request from the VA. The report shall include asset management detail in a sortable MS Excel spreadsheet(s).

Deliverables:

A. EVS PoC Change Review Meeting Agenda Template
B. EVS PoC Change Review Meeting Agenda
C. EVS PoC Change Review Meeting Minutes Template

D. EVS PoC Change Review Meeting Minutes
E. EVS PoC Change Schedule Template
F. EVS PoC Change Schedule
G. EVS PoC Change Management Procedures Template
H. EVS PoC Change Management Procedures
I. EVS PoC Maintenance Window List Template
J. EVS PoC Maintenance Window List
K. EVS PoC Configuration Management Procedures Template
L. EVS PoC Configuration Management Procedures
M. EVS PoC Configuration Management Audit Report Template
N. EVS PoC Configuration Management Audit Report
O. EVS PoC Configuration Management Detail Report
P. EVS PoC Asset Management Procedures Template
Q. EVS PoC Asset Management Procedures
R. EVS PoC Asset Management Audit Report Template
S. EVS PoC Asset Management Audit Report
T. EVS PoC Asset Management Detail Report(s)

5.3.6 PERFORMANCE MANAGEMENT

Performance Management processes are used to ensure EVS PoC provides the level of service required to fulfill VA business needs.

5.3.6.1 SERVICE LEVEL MANAGEMENT

Service Level Management provides the business with the agreed service targets and the required management information to ensure that those targets have been met. This includes implementation of improvement measures for the level of service delivered.

The Contractor shall ensure that changes meet and maintain EVS PoC service level requirements. The Contractor shall monitor, measure, analyze, and evaluate EVS PoC service performance. The Contractor shall optimize EVS PoC service performance. The Contractor shall develop and implement service performance plans to prevent or remediate EVS PoC service performance issues. The Contractor shall include applicable Service Level Management data in the EVS PoC weekly and monthly operations reports.

5.3.6.2 AVAILABILITY MANAGEMENT

Availability Management ensures EVS PoC services are available when VA needs them. This function includes ensuring that the system uptime requirements documented in EVS PoC service level agreements (SLA) are met and that monitoring services are in place per the SLA to proactively respond to projected system demands. Monitoring also provides capacity trending, allowing proactive system modifications or planning for upgrades. This process can make use of a variety of methods to optimize availability.

The Contractor shall monitor, measure, analyze, and report on all aspects of the availability of EVS PoC services. The Contractor also shall analyze, and report on the availability of IT infrastructure, processes, tools, etc. that support EVS PoC. The Contractor shall investigate unavailability, and conduct weekly availability reviews. The Contractor shall develop and publish EVS PoC Availability Management Procedures.

The procedures shall describe the steps for collecting, analyzing, and reporting availability data. A draft procedures template shall be delivered 60 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.6.3 CAPACITY MANAGEMENT

Capacity Management ensures all current and future EVS PoC capacity and performance aspects of the business requirements are provided cost effectively. Furthermore, the goal of Capacity Management is to plan and implement the appropriate EVS PoC capacity while ensuring that EVS PoC services achieve expected levels of performance.

Capacity Management encompasses three sub-processes; Resource Capacity Management, Service Capacity Management, and Business Capacity Management.

- EVS PoC Resource Capacity Management defines resources as computer and computer-related equipment, software, licenses, circuits, facilities, or organization (people). The process focuses on the management of individual components of EVS PoC infrastructure through monitoring, measurement, analysis, and reporting.
- EVS PoC Service Capacity Management defines service as one or more EVS PoC processes that enable a business process. The process focuses on the management of the performance of EVS PoC services through monitoring, measurement, analysis, and reporting.
- Business Capacity Management is responsible for ensuring that both current and future, and strategic and tactical business requirements for EVS PoC service capacity are considered, planned, and implemented.

The Contractor shall increase the capacity of the EVS PoC by 15% each year during the period of performance over the as built design capacity. The Contractor shall monitor, measure, analyze, and report on EVS PoC resource, service, and business capacity usage. The Contractor also shall analyze, and report on the capacity of IT infrastructure, processes, tools, etc. that support EVS PoC. The Contractor shall investigate capacity issues, and conduct weekly capacity reviews. The Contractor shall recommend, plan, and initiate service and resource tuning to optimize EVS PoC capacity. The Contractor shall identify and forecast EVS PoC capacity needs.
The Contractor shall develop and publish EVS PoC Capacity Management Procedures. The procedures shall include step-by-step instructions for collecting, analyzing, and reporting capacity data. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop an EVS PoC Quarterly Capacity Plan. The plan shall contain details of current and historic usage of EVS PoC services and components, and

any issues that need to be addressed (including related improvement activities). The plan also shall contain scenarios for different predictions of business demand and costed options to deliver the agreed service level targets. A draft EVS PoC Capacity Plan template shall be delivered 90 days after contract award. A final plan template shall be delivered 30 days after the Contractor has received comments from the VA. A draft plan shall be delivered 60 days after the template has been finalized. The initial capacity plan shall be delivered 30 days after the Contractor has received comments from the VA. Subsequent capacity plans shall be delivered by the 15th day of each calendar quarter.

Deliverables:

A. EVS PoC Service Performance Plan(s)
B. EVS PoC Availability Management Procedures Template
C. EVS PoC Availability Management Procedures
D. EVS PoC Capacity Management Procedure Template
E. EVS PoC Capacity Management Procedures
F. EVS PoC Quarterly Capacity Plan Template
G. EVS PoC Quarterly Capacity Plan

5.3.7 SECURITY MANAGEMENT

Security Management has overall responsibility for setting policies, standards and procedures to ensure the protection of the organization's assets, data, information and IT services from harm due to failures of confidentiality, integrity and availability; meets security requirements of the business (documented in SLAs and external requirements); and provides a basic level of security (security baseline).
The Contractor shall assess identified vulnerabilities to determine the potential impact of the risk to the EVS PoC environment and advise VA of the recommended mitigation or remediation options. The Contractor shall conduct all OMAPR functions in accordance with the EVS PoC System Security Plan, attached.

The Contractor shall develop and maintain an EVS PoC Security Management Task Schedule for all reoccurring security management tasks that are mandatory or recommended by the manufacturer. The document shall specify the frequency of each task and include, as appropriate, when the task must be executed (e.g., time of day, day of week, or day of month). The document shall identify, for each task, if the task is automated or manual. Automated means "fully" automated to include the starting and stopping of the task. Manual means any task that, in whole or in part, requires a human to perform an action. A draft task schedule template shall be delivered 60 days after contract award. A final task schedule template shall be delivered 30 days after the Contractor has received comments from the VA. A draft task schedule shall be delivered 30 days after the template has been finalized. A final task schedule shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall log completion of all reoccurring security management tasks. The Contractor shall develop and maintain an EVS PoC Security Management Task Log. The log shall include a list of all security management tasks. For each manual task in the log, the Contractor shall record the date and time the task was completed, and the name of the person that completed the task. For each automated task in the log with an

automated mechanism to report failed tasks, no log entry is required. For each automated task in the log without an automated mechanism to report failed tasks, the Contractor shall record the date and time the task was completed, and the name of the person that verified the task completed successfully. A draft log template shall be delivered 90 days after contract award. A final log template shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall annotate completion of tasks in the log per the EVS PoC Security Management Task Schedule.

The Contractor shall develop and maintain an EVS PoC Security Management Task Procedures document for all reoccurring application administration tasks that are manual. The procedures document shall include step-by-step procedures to execute each task. The procedures shall include the expected response, if any, from an application after each step or command is executed. The procedures shall be specific for each type and version of application utilized in EVS PoC. The EVS PoC Security Management Task Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Security Management Task Procedures document. A draft procedures template shall be delivered 90 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.7.1 ACCESS MANAGEMENT

Access management allows users to make use of EVS PoC services, data or other assets. Access Management helps to protect the confidentiality, integrity, and availability of EVS PoC information assets by ensuring that only authorized users are able to access or modify them. The Contractor shall perform Access Management for service provided from the EVS PoC Core.

The Contractor shall implement, administer, and monitor access to EVS PoC Core systems, data, and services according to The VA Information Security Program and per the specific access controls authorized for EVS PoC. The Contractor shall recommend changes to EVS PoC access controls. The Contractor shall develop and maintain procedures for granting, modifying, terminating, and auditing access to EVS PoC Core systems, data, and services. The Contractor shall update these procedures on an as needed basis. The Contractor shall audit all EVS PoC Core access accounts annually, notify VA of any accounts that do not meet VA or EVS PoC security policies or standards, and remediate EVS PoC access accounts as directed by VA.

The EVS PoC Access Management Procedures document shall include procedures for granting, modifying, and terminating access for each type of EVS PoC Core access account. The procedures shall be specific for each type and version of hardware/software on which EVS PoC Core access accounts are configured. The document also shall include procedures for auditing EVS PoC Core access accounts against VA, OI&T and EVS PoC information security policies, standards, and controls. The audit procedures shall include hardware/software specific steps used to export EVS PoC account data necessary to conduct an audit. The procedures shall include the

expected response, if any, after each step or command is executed. A draft document template shall be delivered 30 days after contract award. A final document template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedure document shall be delivered 30 days after the template has been finalized. A final procedure document shall be delivered 30 days after the Contractor has received comments from the VA.

The contractor shall provide an EVS PoC Access Management Annual Audit Report. The report shall include a summary of the total number of physical and virtual devices in the EVS PoC Core; the number and percentage of EVS PoC Core physical and virtual devices with access accounts; the total number of EVS PoC Core access accounts; the number of EVS PoC Core access accounts for each access account type and the percentage of the EVS PoC Core access account total for each access account type; the total number of EVS PoC Core access accounts that do not comply with VA, OI&T, or EVS PoC policies, standards, or controls; the number of EVS PoC Core access accounts by type that do not comply with VA, OI&T, or EVS PoC policies, standards, or controls and the percentage of the total that do not comply. The report shall include or reference a complete list of all EVS PoC Core physical and virtual devices with access accounts. The report shall include a list of all EVS PoC Core access accounts that do not comply with VA, OI&T, or EVS PoC policies, standards, or controls, the EVS PoC Core physical or virtual device(s) on which the account is configured, the reason why each account is non-compliant, and a recommended remediation action for each account. A draft report template shall be delivered 30 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from the VA. A draft report shall be delivered January 10th of each calendar year. A final report shall be delivered January 31st of each calendar year.

The contractor shall provide an EVS PoC Access Management Remediation Report annually. The report shall include a summary of the total number of EVS PoC Core access accounts recommended for remediation in the most recent EVS PoC Access Management Audit Report, and the number of EVS PoC Core access accounts that were remediated. The report shall include a list of any EVS PoC Core access accounts recommended for remediation, but were not remediated, and the reason why the account was not remediated. A draft report template shall be delivered 60 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from the VA. A draft report shall be delivered February 15th of each calendar year. A final report shall be delivered each calendar year, 15 days after the Contractor has received comments from VA.

5.3.7.2 ASSESSMENT & AUTHORIZATION (A&A)

The EVS PoC solution must meet VA security mandates, and obtain and retain an Authority to Operate (ATO); via VA's A&A process. Currently, the EVS PoC has a Temporary Authority to Operate (TATO) and is expected to receive an ATO prior to award of this contract. Completion of the initial, or renewal of a subsequent, EVS PoC A&A process requires developing policies, procedures, and technical controls based upon guidelines such as VA 6500 Policy Handbook and NIST 800-53 rev4. The Contractor shall support development of A&A artifacts for the initial ATO if needed as assigned by VA.

The Contractor shall update required A&A documentation and provide supporting evidence that security controls are in place as needed when changes to EVS PoC occur. Required supporting documents include, but are not limited to, System Security Plan, Information Security Policy, Audit Management Policy, Account Management Policy, Privacy Impact Assessment, Incident Response Plan, Information Security Contingency Plan, Configuration Management Plan, and Disaster Recovery Plan. The Contractor shall provide all necessary support in completion of the EVS PoC A&A package to maintain or renew an ATO. The Contractor shall provide remediation to correct any vulnerabilities identified by the VA.

5.3.7.3 AUDIT RECORDS

The Contractor shall allocate audit record storage capacity and configure auditing to prevent audit record storage capacity being exceeded for EVS PoC Core auditable events. The Contractor shall, on a weekly basis, review and analyze EVS PoC Core audit records for indications of inappropriate or unusual activity, and report findings to VA in the EVS PoC Weekly Operations Report.

5.3.7.4 EMERGENCY POWER SHUTDOWN

When notified of the loss of primary power for EVS PoC systems, the Contractor shall facilitate, as needed and with VA authorization, an orderly/graceful shutdown of the EVS PoC systems affected to prevent system damage, or loss or corruption of data. The Contractor shall develop and maintain an EVS PoC Emergency Shutdown Procedures document. The procedures document shall include step-by-step procedures for each EVS PoC component that requires an orderly/graceful shutdown. The procedures shall include the expected response, if any, from the system after each step or command is executed. The procedures shall be specific for each type and version of system utilized in EVS PoC. The EVS PoC Emergency Shutdown Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Emergency Shutdown Procedures document. The document also shall include procedures for restarting EVS PoC systems once power has been restored. The document also shall list the EVS PoC systems that do not require an orderly/graceful shutdown. A draft procedures template shall be delivered 120 days after contract award. A final procedures template shall be delivered 30 days after the Contractor has received comments from the VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.7.5 EQUIPMENT MOVEMENT

The Contractor shall obtain approval from the VA EVS PoC Project Manager or designee, prior to relocating any EVS PoC Core equipment; e.g., returning/shipping equipment to the manufacturer or other 3rd party as part of a support contract, or disposing of equipment in any other manner. The Contractor shall ensure sanitization of EVS PoC Core equipment to remove all information from associated media prior to removal from VA facilities.

5.3.7.6 MAINTENANCE AND REPAIR

The Contractor shall check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. The Contractor shall ensure that maintenance records for EVS PoC include: the date and time of maintenance; name of the individual performing the maintenance; name of escort, if necessary; a description of the maintenance performed; and a list of equipment removed or replaced (including identification numbers, if applicable). As part of the EVS PoC change process, the Contractor shall update the EVS PoC System Design Document and other applicable Assessment & Authorization documentation as needed. The Contractor shall identify and notify VA, prior to change approval, whenever a change to EVS PoC requires a new Assessment & Authorization, and ATO. As part of the EVS PoC change process, the Contractor shall assist with updating applicable RiskVision and Continuity Database data and documents. The Contractor shall identify and notify VA, prior to change approval, whenever a change to EVS PoC requires updates in RiskVision or the Continuity Database.

5.3.7.7 SECURITY INCIDENT RESPONSE

The Contractor shall immediately report suspected or confirmed network intrusions and/or data breaches to the VA NSOC, EVS PoC Project Manager, and EVS PoC ISO. The Contractor shall fully participate in incident preparation, detection, reporting, analysis, corrective/mitigation, and post incident activities. VA has a security information and event management (SIEM) solution. EVS PoC does not require SIEM beyond what VA currently has in place.

The Contractor shall develop and maintain an EVS PoC Security Incident Notification and Escalation List and Procedures document. The document shall contain primary and alternate contacts and contact methods for each organization or individual required to be notified if the Contractor discovers an intrusion or breach, or if the Contractor is notified by another organization or individual that an EVS PoC intrusion or breach has occurred. The document shall describe the procedures the Contractor shall execute during the initial notification or notification escalation. A draft document template shall be delivered 30 days after contract award. A final document template shall be delivered 15 days after the Contractor has received comments from the VA. A draft document shall be delivered 15 days after the template has been finalized. A final document shall be delivered 15 days after the Contractor has received comments from the VA. The Contractor shall audit the EVS PoC Security Incident Notification and Escalation List and Procedures document on a quarterly basis, and update the contents as needed.

5.3.7.8 STORAGE MEDIA

The Contractor shall ensure that removable information system media and information system output is marked indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; except for specific types of media or hardware, as documented in the system security plan, such as disk packs and backup tapes, as long as the exempted items remain within the secured computer room.

For media under the Contractor’s control, the Contractor shall physically control and securely store information systems media, both paper and electronic, within VA

approved controlled areas based on the highest FIPS 199 security category of the information recorded on the media; and protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

The Contractor shall protect and control information system media, paper and electronic, during transport outside of controlled areas using security measures that protect the items from disclosure, compromise, or breach. The Contractor shall maintain accountability for information system media during transport outside of controlled areas; and shall restrict the activities associated with transport of such media to authorized personnel. The Contractor shall document activities associated with the transport of information system media. The Contractor shall employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

5.3.7.9 INFORMATION TECHNOLOGY SERVICE CONTINUITY MANAGEMENT (ITSCM)

The purpose of ITSCM is to support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and service desk) can be recovered within required and agreed-upon business timescales. ITSCM ensures that appropriate continuity mechanisms are in place and detailed in the Information System Contingency Plan (ISCP) for EVS PoC. An ISCP is usually incorporated into or referenced in Disaster Recovery Plans (DRP), Business Continuity Plans (BCP), and Continuity of Operations Plans (COOP).

The Contractor shall monitor, assess and maintain EVS PoC service continuity capabilities. The Contractor shall develop, update, and publish EVS PoC ISCPs and related training plans and materials, test plans, exercise plans, and checklists. The Contractor shall train, test, exercise, evaluate, and execute information system contingency plans (ISCPs) for EVS PoC. The Contractor shall recommend, plan, initiate, and implement changes to optimize or enhance EVS PoC service continuity capabilities.

The Contractor shall provide support to VA to integrate EVS PoC ISCPs into DRPs, BCPs, COOPs, and the VA Comprehensive Emergency Management Program. This includes remotely implementing and supporting EVS PoC systems and services, for use in COOP implementation, within 12 hours of COOP activation and to be sustained for up to 30 days. The Contractor shall manage execution of EVS PoC Core ISCPs. The Contractor shall participate in the execution of EVS PoC ISCPs for the Distribution and Local EVS PoC architecture layers. The Contractor shall participate in VA continuity tests, training, exercises, and evaluations as directed by VA. The Contractor shall provide necessary data elements required by VA’s Information System Contingency Planning Assessment (ISCPA) tool in conjunction with supporting the Assessment and Authorization (A&A) process for EVS PoC.

5.3.7.9.1 INFORMATION SYSTEM CONTINGENCY PLANS

The Contractor shall review and update ISCPs for the EVS PoC Cores a minimum of once annually. EVS PoC ISCPs shall address all failure scenarios that can impact EVS

PoC services, including failures caused by non-EVS PoC components such as LAN or WAN. The Contractor shall design EVS PoC ISCPs to provide the minimum agreed EVS PoC service levels during recovery of EVS PoC systems and services. Each EVS PoC ISCP shall include detailed steps required to recover EVS PoC systems and services. Each EVS PoC ISCP shall include the trigger(s) for invocation. Each ISCP shall document the roles and responsibilities of organizations and individuals involved in managing and executing the ISCP. The Contractor shall provide support to Service Lines and sites as required to update ISCPs for EVS PoC Distribution or Local architecture layers.

VA consolidates Information System Contingency Planning within a structured, multi-stage questionnaire in VA's Continuity Database (CDB). The Contractor either shall directly update VA's CDB, or provide EVS PoC ISCP data in the format that is easily inserted into the CDB by Service Line or Site EVS PoC support personnel.

The Contractor shall create and maintain an EVS PoC Consolidated ISCP Performance Targets list of all EVS PoC maximum tolerable downtime (MTD), recovery time objective (RTO) and recovery point objective (RPO) targets determined by Information System Contingency Planning Assessments (ISCPA). The list also shall include global MTD, RTO, and RPO specified by VA, OI&T, or EVS PoC. The list shall include location; e.g., city, state, Active Directory abbreviation, station ID; and organizational; e.g., Region, VISN, MSN; information. A draft list template shall be delivered 150 days after contract award. A final list template shall be delivered 30 days after the Contractor has received comments from the VA. A draft list shall be delivered 30 days after the template has been finalized. The initial list shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.7.9.2 ISCP TRAINING

The Contractor shall develop and maintain ISCP training plans and materials for the EVS PoC Cores. The training plans and materials shall adequately educate and prepare organizations and individuals on their roles and responsibilities in managing and executing EVS PoC ISCPs. VA utilizes an enterprise wide Talent Management Systems (TMS) to deliver and track web based training. The Contractor shall provide multimedia EVS PoC ISCP training materials that can be integrated into TMS. The Contractor shall coordinate with the TMS administrator to publish EVS PoC ISCP training materials in TMS. The Contractor shall annually train their EVS Helpdesk personnel on their ISCP roles and responsibilities. The Contractor shall update EVS PoC ISCP training plans and materials, and retrain their staff when a significant change, as determined by VA, is made to an EVS PoC ISCP.

A draft EVS PoC ISCP Training Plan template shall be delivered 150 days after contract award. A final EVS PoC ISCP Training Plan template shall be delivered 30 days after the Contractor has received comments from the VA. A draft training plan shall be delivered 30 days after the template has been finalized. The initial training plan shall be delivered 30 days after the Contractor has received comments from the VA.

Draft TMS compatible EVS PoC ISCP training materials shall be delivered 210 days after contract award. TMS compatible EVS PoC ISCP training materials shall be delivered 30 days after the Contractor has received comments from the VA.

5.3.7.9.3 ISCP TESTS AND EXERCISES

The Contractor shall conduct an EVS PoC ISCP Test and an EVS PoC ISCP Exercise on the EVS PoC Core systems annually. The Contractor shall conduct the test and exercise at different times of the year. At the discretion of VA, each EVS PoC ISCP Exercise may be either a tabletop exercise (TTX), a command post exercise (CPX), or a full function / field training exercise (FTX). The Contractor shall participate in ISCP, DRP, BCP, and COOP tests and exercises conducted by other VA organizations, of which EVS PoC is a component.

- EVS PoC ISCP Test Minimum Requirements
    - Test alert, notification, and activation procedures for EVS PoC ISCP personnel.
    - Test procedures for recovering EVS PoC systems, services, and data.

- EVS PoC ISCP Exercise Minimum Requirements
    - Allow opportunity for EVS PoC ISCP personnel to demonstrate familiarity with ISCP plans and procedures.
    - Allow opportunity to demonstrate that EVS PoC backup data is sufficient, complete, and current.
    - Allow opportunity for EVS PoC ISCP personnel to demonstrate their familiarity with the EVS PoC reconstitution procedures to transition from an EVS PoC recovery environment to a normal EVS PoC environment.

The Contractor shall develop an EVS PoC ISCP Test Plan. The document shall specify the roles and responsibilities of test participants. The test plan shall specify what is to be tested, how it is to be tested and expected test results. The test plan shall include a score card to be used to record the test results. A draft test plan template shall be delivered 150 days after contract award. A final test plan template shall be delivered 30 days after the Contractor has received comments from the VA. A draft test plan shall be delivered 30 days after the template has been finalized. A final test plan shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop an EVS PoC ISCP Exercise Plan. The plan shall include sequencing, checklists, and expected results. The document shall specify the roles and responsibilities of exercise participants. A draft exercise plan template shall be delivered 150 days after contract award. A final exercise plan template shall be delivered 30 days after the Contractor has received comments from the VA. A draft exercise plan shall be delivered 30 days after the template has been finalized. A final exercise plan shall be delivered 30 days after the Contractor has received comments from the VA.

The Contractor shall develop an EVS PoC ISCP Test Report. The report shall be comprehensive and identify weaknesses in plans and procedures. The report shall recommend revisions and include a POA&M. A draft report template shall be delivered 150 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from the VA. The Contractor shall provide an EVS PoC ISCP Test Report within 14 days after each test. The Contractor shall develop an EVS PoC ISCP Exercise Report. The report shall be comprehensive and identify weaknesses in plans, processes, procedures, products, partners, and people. The

report shall recommend changes and include a POA&M. A draft report template shall be delivered 150 days after contract award. A final report template shall be delivered 30 days after the Contractor has received comments from VA. The Contractor shall provide an EVS PoC ISCP Exercise Report within 14 days after each exercise.

5.3.7.9.4 ISCP RESPONSE AND EXECUTION

The Contractor shall initiate the relevant EVS PoC ISCP when notified by the appropriate authority that an ISCP, DRP, BCP, or COOP has been activated which involves EVS PoC or which requires support from EVS PoC. In the event that an EVS PoC degradation or outage may, or will, exceed the maximum tolerable down-time (MTD) for an EVS PoC customer, the Contractor shall promptly coordinate with VA to authorize and activate the appropriate EVS PoC ISCP.

Deliverables:

A. EVS PoC Security Management Task Schedule Template
B. EVS PoC Security Management Task Schedule
C. EVS PoC Security Management Task Log Template
D. EVS PoC Security Management Task Procedures Template
E. EVS PoC Security Management Task Procedures
F. EVS PoC Access Management Procedures Template
G. EVS PoC Access Management Procedures
H. EVS PoC Access Management Annual Audit Report Template
I. EVS PoC Access Management Annual Audit Report
J. EVS PoC Access Management Remediation Report Template
K. EVS PoC Access Management Remediation Report
L. EVS PoC Weekly Audit Record Report
M. EVS PoC Security Incident Notification and Escalation List and Procedures Template
N. EVS PoC Security Incident Notification and Escalation List and Procedures
O. EVS PoC Emergency Shutdown Procedures Template
P. EVS PoC Emergency Shutdown Procedures
Q. EVS PoC Consolidated ISCP Performance Targets Template
R. EVS PoC Consolidated ISCP Performance Targets
S. EVS PoC Core ISCP
T. EVS PoC ISCP Training Plan Template
U. EVS PoC ISCP Training Plan
V. EVS PoC ISCP Training Materials (compatible with TMS)
W. EVS PoC ISCP Test Plan Template
X. EVS PoC ISCP Test Plan
Y. EVS PoC ISCP Test Report Template
Z. EVS PoC ISCP Test Report
AA. EVS PoC ISCP Exercise Plan Template
BB. EVS PoC ISCP Exercise Plan
CC. EVS PoC ISCP Exercise Report Template
DD. EVS PoC ISCP Exercise Report

5.3.8 KNOWLEDGE MANAGEMENT

Knowledge Management gathers, analyzes, stores, and shares knowledge; which reduces the need to re-discover knowledge. Knowledge Management ensures that, at any given time and location, users and service support personnel have adequate and accurate information; allowing them to be more efficient. Knowledge Management helps improve quality of service, increase satisfaction, and reduce cost. The Contractor shall perform Knowledge Management for EVS PoC.

The Contractor shall, create/update, evaluate/review, edit, and publish EVS PoC knowledge documents. The Contractor shall audit EVS PoC knowledge documents annually. The Contractor shall keep EVS PoC knowledge documents current as changes are made to the EVS PoC environment. The Contractor shall relocate existing EVS PoC knowledge documents from their current EVS Helpdesk SharePoint site to a new EVS Helpdesk SharePoint site. The Contractor shall move the EVS PoC knowledge documents within 30 days after the new repository is identified. The expected quantity of EVS PoC knowledge documents at time of contract award is provided in the following table.

Table 5.11 – EVS PoC Knowledge Document Counts

EVS Helpdesk Repository	
NSD Repository	

5.4 OPTIONAL TASKS

5.4.1 OPTIONAL: MACD LOCAL LEVEL SUPPORT

The Contractor shall perform Moves, Adds, Changes, and Disconnects support at the sites. Soft MACDs such as password changes, button/feature adds, changes or removal, or other software-only type changes shall also be performed by the Contractor. Any MACD involving the Contractor shall be trackable and auditable in the National Service Desk ticketing system with detail such as type of MACD requested, activities performed and by whom, and timestamps. The number of MACD requests opened, completed, timestamps, type of MACD, action taken, and completion date shall be provided as part of the Monthly Progress and Performance Report.

The table below provides average numbers of physical moves, adds, changes, and disconnects by local site.

Site	Average Number of Monthly Physical
Ft. Harrison, MT	60
TN Valley Healthcare	80
Charleston, SC	30

5.4.2 OPTIONAL: SITE ACTIVATION SUPPORT

The Contractor shall provide support in the activation of EVS PoC at new facilities associated with the existing EVS PoC sites. Examples of new facilities may be Veterans Centers, Community Based Outpatient Clinics, and research or administrative service

locations. Support provided under this CLIN should include all work required to configure, test, install and activate EVS PoC-related capabilities, as specified in Addendum D, at a new facility.

New facilities must be designed and configured with the same level of performance; e.g. call quality, and call capacity; as similar existing EVS PoC facilities. The design and configuration of a new facility must take into consideration any changes to the existing EVS PoC system that are required to support the facility, including but not limited to software licensing, storage for increased Call Detail Records, etc. VA will work in conjunction with the Contractor to determine infrastructure requirements necessary to successfully implement the activation, and will provide all necessary equipment (hardware and software) and licenses. The Contractor shall update EVS PoC documents; e.g., design and security; with any implemented changes.

5.4.3 OPTIONAL: MOVE VOICEMAIL FROM CORES TO SITES

The Contractor shall support implementation moving existing voicemail from existing Core systems to the EVS PoC sites. Contractor shall evaluate existing EVS PoC site systems, available capacity, and produce a change management and transition plan to migrate voicemail from cores to existing site EVS PoC servers. VA will work in conjunction with the Contractor to determine infrastructure requirements necessary to successfully implement the activation, and will provide all necessary equipment (hardware and software) and licenses. Contractor shall schedule voice mail migration and provide end user support.

Contractor shall deliver a Voicemail Migration Plan for each site within 60 days of exercise of option.

Deliverables:

A. Voicemail Migration Plan for Ft. Harrison
B. Voicemail Migration Plan for Charleston
C. Voicemail Migration Plan for Tennessee Valley

5.4.4 OPTIONAL: CORE AND DISTRIBUTION LAYER EXPANSION SUPPORT

The Contractor shall provide support in the expansion of EVS to include (2) two additional EVS Core sites and EVS Regional Distribution architecture capability and capacity beyond the existing EVS PoC sites. Examples of core and distribution layer expansion support would include administrative, operations and maintenance of the hardware and software consistent and fully compatible with the EVS PoC cores. Support provided under this task should include all work required to configure, test, and integrate the expansion into the existing Architecture. All contractor work for this task will be able to be accomplished remotely from the EVS Helpdesk. The Contractor is responsible for the design, configuration, testing, or installation of the expanded Core or Distribution components.

Contractor shall manage and operate the new core components at the same level of performance, e.g. call quality and call capacity, as similar existing EVS installations. The new core and distribution layer functionality will include transitioning the EVS PoC sites from the existing core to the appropriate core/distribution layer architecture as directed by VA. The contractor must take into consideration any changes to the existing EVS

PoC system that are required to support these activities including but not limited to software licensing, storage for increased volume of Call Detail Records, etc. VA will work in conjunction with the Contractor to determine infrastructure requirements necessary to successfully implement the activation of new EVS Core and/or Distribution Architecture components, and will provide all necessary equipment (hardware and software) and licenses. The Contractor shall update EVS documents, e.g., design and security, with any implemented changes.

The Contractor shall develop a Site Design Document that includes, but is not limited to, all equipment, integration points, and system interfaces defined. This shall be delivered 30 days after exercise of this option. The Contractor shall develop an As Built Design that includes, but is not limited to, all equipment, integration points, and system interfaces. This shall be delivered within 30 days of VA acceptance of installation.

Deliverables:

A. Site Design (Per Site/Location)

B. As Built Site Design (Per Site/Location)

5.4.5 OPTIONAL: CONVERGED VIRTUAL INFRASTRUCTURE

The Contractor shall support implementation moving existing EVS PoC systems and servers to new Converged Virtual Infrastructure platform. Contractor shall evaluate existing EVS PoC site systems, available capacity, and produce a change management and transition plan to migrate all EVS PoC systems and services from existing site EVS PoC servers to new Converged Virtual Infrastructure servers. Contractor shall schedule system migration and provide end user support.

Contractor shall deliver a System Migration Plan for each site within 60 days of exercise of option.

Deliverables:

C. System Migration to CVI for Ft. Harrison
D. System Migration to CVI for Charleston
E. System Migration to CVI for Tennessee Valley

5.4.6 OPTIONAL: ACTIVITIES SUPPORTING INTEGRATION WITH IPv6

The Contractor shall support implementation of IPv6 capabilities and features in EVS PoC. IPv6 integration shall include but not be limited to support for IPv6 addressing management schemes, DHCPv6 and IPv6 routing. Contractor solution shall comply with all IPv6 Federal mandates and directives. The Contractor IPv6 solution shall take into consideration the existing VA IPv4 networks where applicable to include running dual stack. The Contractor shall update EVS PoC documents, e.g., design and security, with any IPv6 changes. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. IPv6 Design and Approach

5.4.7 OPTIONAL: INTEGRATION WITH VA ENTERPRISE UC APPLICATIONS

5.4.7.1 OPTIONAL VANTS INTEGRATION

The Contractor solution shall support audio integration between EVS PoC and VA's Nationwide Teleconferencing System's (VANTS) audio and video teleconferencing bridges. This includes, but is not limited to, activities such as planning, design, configuration, testing, and deployment within the EVS PoC architecture. The Contractor shall coordinate with the VANTS team and other VA organizations as need to complete this task. The Contractor is not responsible for design, configuration, or deployment within the VANTS architecture. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. VANTS Integration Design and Approach

5.4.7.2 OPTIONAL LYNC INTEGRATION

Contractor EVS PoC Sustainment solution shall support integration with VA's existing Microsoft Lync, which provides an instant messaging client used with Microsoft Lync Server providing Voice Over IP (VOIP), video conferencing and application sharing capabilities. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. MS Lync Integration Design and Approach

5.4.7.3 OPTIONAL EVTN INTEGRATION

The Contractor solution shall support audio and presence integration with VA's Enterprise Video Teleconferencing Network (EVTN), which provides video conferencing capabilities. This includes, but is not limited to, activities such as planning, design, configuration, testing, and deployment within the EVS PoC architecture. The Contractor shall coordinate with VA's EVTN team and other VA organizations as need to complete this task. The Contractor is not responsible for design, configuration, or deployment within the EVTN architecture. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. EVTN Integration Design and Approach

5.4.7.4 OPTIONAL LOCAL 3rd PARTY APPLICATION INTEGRATION

The Contractor solution shall support audio integration with other applications, e.g., nurse call, dictation, land-mobile radio, installed at EVS PoC locations. This includes, but is not limited to, activities such as planning, design, configuration, testing, and deployment within the EVS PoC architecture. The Contractor shall coordinate with VA

organizations as need to complete this task. The Contractor is not responsible for design, configuration, or deployment of the other application. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. Local Application Integration Design and Approach

5.4.7.5 OPTIONAL Other UC APPLICATION INTEGRATION

The Contractor solution shall support audio integration with other unified communications (UC) applications. This includes, but is not limited to, activities such as planning, design, configuration, testing, and deployment within the EVS PoC architecture. The Contractor shall coordinate with VA organizations as need to complete this task. The Contractor is not responsible for design, configuration, or deployment of the other application. The contractor shall update all EVS PoC documents (e.g., design, security, and approach) as the application technology changes.

Deliverables:

A. Unified Communication Integration Design and Approach

5.4.8 OPTIONAL: INCREMENTAL EQUIPMENT PURCHASE

The Contractor shall provide pricing for telephone devices in quantities of 1, 10, 25, and 100 units. The proposed equipment will be the same model(s) as those being maintained. If the models being maintained have reached End of Sale, the newest version/fully featured compatible, TAA compliant model shall be available upon VA approval. The Contractor shall ensure all manufacturer supportable EVS PoC configuration items, e.g., hardware and software, purchased via this task are under a manufacturer support contract per the requirements listed in tables D.2 and D.3 in Addendum D, Section D.1.1.1.

5.4.9 OPTIONAL: CAPACITY AUGMENTATION

Within 30 days of exercise of option, the Contractor shall provide a cost estimate for EVS PoC capacity increases specified by VA. The cost estimate shall be inclusive of any EVS PoC components (e.g. hardware, software, licenses, PSTN connections). The Contractor may be required to provide a cost estimate no more frequently than once per quarter (90 days).

Deliverables:

A. EVS PoC Capacity Augmentation Cost Estimate

5.4.10 OPTIONAL: DATABASE ADMINISTRATION

Database Administration schedules database tasks, develops backup schedules, monitors operations of databases, and troubleshoots the database when a problem occurs. In addition, Database Administration participates in tuning the database to

resolve performance issues. The Contractor shall perform Database Administration for EVS PoC.

The Contractor shall monitor EVS PoC databases for security, performance, fault, and configuration issues. The Contractor shall identify negative trends and repetitive issues, and notify VA. The Contractor shall optimize database performance, and shall recommend and implement changes to prevent or remediate database performance issues. The Contractor shall include applicable Database Administration data in the EVS PoC weekly and monthly operations reports.

The Contractor shall monitor OEM tech bulletins for database releases, bugs, vulnerabilities, fixes, patches, and end-of-life notices. OEM includes any free or licensed databases embedded within EVS PoC software. The Contractor also shall monitor U.S. CERT and VA NSOC bulletins for vulnerabilities in EVS PoC databases and related software. The Contractor shall identify, recommend, and implement database upgrades or patches necessary to remediate vulnerabilities or bugs. The Contractor shall identify, recommend, and implement database upgrades and patches for EVS PoC databases and related software with an OEM end-of-life notice, or forecasted to be deprecated per the One-VA Technical Reference Model (TRM).

The Contractor shall schedule and conduct database backups or synchronization that meet EVS PoC information system contingency plan and disaster recovery plan targets; including, but not limited to, recovery time objectives and recovery point objectives. At a minimum, the Contractor shall perform database backups daily or real-time with real-time mirroring/shadowing. At a minimum, the Contractor shall perform database documentation backups annually. At a minimum, the Contractor shall test database backup information to verify media reliability and information integrity weekly. At a minimum, the Contractor shall test database documentation backup information to verify media reliability and information integrity quarterly.

The Contractor shall forecast system storage needs for EVS PoC databases, and shall notify VA 18 months prior to an EVS PoC database projected to be impacted by any storage limits. Storage includes internal EVS PoC system storage and any storage external to EVS PoC systems that is utilized for EVS PoC databases. The Contractor shall request and/or provision additional storage for EVS PoC databases in sufficient time to prevent EVS PoC services from being impacted by storage limits.

The Contractor shall develop, implement, and maintain database operational scripts. The Contractor shall maintain Record of Database Operational Event Logs, and shall perform data restoration activities, and shall request vendor support for database issues.

The Contractor shall develop and maintain an EVS PoC Database Administration Task Schedule for all reoccurring database administration tasks that are mandatory or recommended by the manufacturer; or by VA, OI&T or EVS PoC policies or standards. The document shall specify the frequency of each task and include, as appropriate, when the task must be executed (e.g., time of day, day of week, or day of month). The document shall identify, for each task, if the task is automated or manual. Automated means “fully” automated to include the starting and stopping of the task. Manual means any task that, in whole or in part, requires a human to perform an action. A draft task

schedule template shall be delivered 30 days after exercise of option. A final task schedule template shall be delivered 30 days after the Contractor has received comments from VA. A draft task schedule shall be delivered 30 days after the template has been finalized. A final task schedule shall be delivered 30 days after the Contractor has received comments from VA.

The Contractor shall log completion of all reoccurring database administration tasks. The Contractor shall develop and maintain an EVS PoC Database Administration Task Log. The log shall include a list of all database administration tasks. For each manual task in the log, the Contractor shall record the date and time the task was completed, and the name of the person that completed the task. For each automated task in the log with an automated mechanism to report failed tasks, no log entry is required. For each automated task in the log without an automated mechanism to report failed tasks, the Contractor shall record the date and time the task was completed, and the name of the person that verified the task completed successfully. A draft log template shall be delivered 30 days after exercise of option. A final log template shall be delivered 30 days after the Contractor has received comments from VA.

The Contractor shall develop and maintain an EVS PoC Database Administration Task Procedures document for all reoccurring database administration tasks that are manual. The procedures document shall include step-by-step procedures to execute each task. The procedures shall include the expected response, if any, from the database after each step or command is executed. The procedures shall be specific for each type and version of database utilized in EVS PoC. The EVS PoC Database Administration Task Procedures document may reference step-by-step instructions in a suitable manufacturer document, to include section and subsection, in lieu of providing step-by-step instructions directly in the EVS PoC Database Administration Task Procedures document. A draft procedures template shall be delivered 30 days after exercise of option. A final procedures template shall be delivered 30 days after the Contractor has received comments from VA. A draft procedures document shall be delivered 30 days after the template has been finalized. A final procedures document shall be delivered 30 days after the Contractor has received comments from VA.

Deliverables:

A. EVS PoC Database Administration Task Schedule Template
B. EVS PoC Database Administration Task Schedule
C. EVS PoC Database Administration Task Log Template
D. EVS PoC Database Administration Task Procedures Template
E. EVS PoC Database Administration Task Procedures

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise

Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are PIV-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/EAOI&T/OneVA/EAETA.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/docs_design_patterns.asp. The Contractor shall ensure all Contractor delivered applications and systems are compliant with VA Identity Management Policy (VAIQ# 7011145), Continued Implementation of Homeland Security Presidential Directive 12 (VAIQ#7100147), and VA IAM enterprise identity management requirements (IAM Identity Management Business Requirements Guidance document), located at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514. The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with NIST Special Publication 800-63-2, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for both direct and assertion based authentication. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of both Personal Identity Verification (PIV) and Common Access Card (CAC). Assertion authentication at a minimum must include Security Assertion Markup Language (SAML) token authentication and authentication/account binding based on trusted headers. Specific Identity and Access Management PIV requirements are set forth in OMB Memoranda M-04-04 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf), M-05-24 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf), M-11-11 (http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf), National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, and supporting NIST Special Publications. For applications, software, or hardware that cannot support PIV authentication, a Risk Based Decision must be approved by the Deputy Assistant Secretary for Information Security.

(Section 6.1, paragraph 3, below contains the requirement that all Contractor Solutions must support Internet Protocol Version 6 (IPv6)) If the requiring activity has obtained a signed waiver from the VA OI&T CIO office that the IPv6 requirement cannot be met due to patient safety, patient care, or other exception, then the following language (in green), or similar, must replace the IPv6 paragraph 3 below. The requiring activity can modify the green language below as necessary, in accordance with their specific requirements.)

A signed waiver has been obtained from the VA OI&T CIO Office that the IPv6 requirement cannot be met, and as a result, IPv6 is not a requirement for this effort.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf) & (http://www.cybertelecom.org/dns/ipv6usg.htm). IPv6 technology, in accordance with the USGv6: A Technical Infrastructure for USGv6 Adoption (http://www.nist.gov/itl/antd/usgv6.cfm) and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html), shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 users, including all internal infrastructure and applications shall communicate using native IPv6 operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services, in addition to OMB/VA memoranda, can be found at https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 (http://www.dhs.gov/sites/default/files/publications/TIC_Ref_Arch_v2%200_2013.pdf).

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Internet Explorer 11, Office 2013, and Windows 8.1. However, Internet Explorer 11, Office 2013 and Windows 8.1 are not the VA standard yet and are currently not approved for use on the VA Network, but are in-process for future approval by OI&T. Upon the release approval of Internet Explorer 11, Office 2013, and Windows 8.1 individually as the VA standard, Internet Explorer 11, Office 2013, and Windows 8.1 will supersede Internet Explorer 9, Office 2010, and Windows 7 respectively. Applications delivered to VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a 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) specific to the particular client operating system being used.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OI&T Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 POSITION/TASK RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.2.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
Low / Tier 1	**Tier 1 / National Agency Check with Written Inquiries (NACI)** A Tier 1/NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate / Tier 2	**Tier 2 / Moderate Background Investigation (MBI)** A Tier 2/MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High / Tier 4	**Tier 4 / Background Investigation (BI)** A Tier 4/BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check,

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Suitability and Security Program," Appendix A)
	and a verification of the educational degree.

(It is required to identify the appropriate background investigation level (Tier 1/NACI, Tier 2/MBI, Tier 4/BI) by PWS task. Using the results of the Position Designation Automated Tool (PDT) performed by Task, complete the table below. This "Task" Position Risk Designation correlates to individual Contractor personnel background investigation levels depending upon which particular tasks the contractor individual is working.

The PDT Tool is located at the following US Office of Personnel Management Website: http://www.opm.gov/investigate/resources/position/index.aspx)

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

(List PWS Task Section Numbers for this effort (Subsections only as required) in the first column. Double click on the selection box in the appropriate Position Risk Designation column to indicate the proper Risk Designation associated with each task based upon the PDT tool results.)

	Position Sensitivity and Background Investigation Requirements		
Task Number	Tier1 / Low / NACI	Tier 2 / Moderate / MBI	Tier 4 / High / BI
5.1	☐	☒	☐
5.2	☐	☒	☐
5.3	☐	☒	☐
5.3.2.1.4	☐	☐	☒
5.4	☐	☒	☐

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

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the ProPath template. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (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.

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) For a Tier 1/Low Risk designation:
        a) OF-306
        b) DVA Memorandum – Electronic Fingerprints
    2) For Tier 2/Moderate or Tier 4/High Risk designation:
        a) OF-306
        b) VA Form 0710
        c) DVA Memorandum – Electronic Fingerprints
f. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).
g. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the

COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eQIP).

h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or “Closed, No Issues” (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed “Contractor Rules of Behavior.” However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The 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.
k. 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.
l. Identity Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

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

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Performance Levels for Objectives associated with this effort.

(The below standards are generic type standards. When more specific standards can be applied, they should be included within the appropriate "Performance Objective" category row, as a sub-item Standard under the appropriate "Performance Standard" item) (To format the chart-hit the return key after the main "Performance Standard" that requires a sub-item within that Standard, then hit the "Increase Indent" button in the "Home" "Paragraph" toolbar to automatically indent for the sub-item a., b., c., etc.).

Performance Objective	Performance Standards	Acceptable Performance Levels
Effective Communication	No less than 3 contacts per week from Contractor	100% of the time
EVS PoC Services Availability	Maintain EVS PoC Availability 24/7	99.995% or better availability, measured on a monthly basis at the Core/distribution layer; 99.99% at the VAMC facility layer; and 99.9% at VA secondary facilities.
Response to VA Query	Responses received within 8 business hours of request	95% of the time measured on a monthly basis
Required Reports	Submit required reports daily, weekly, monthly, or yearly as prescribed by the PWS	99% of the time measured on a monthly basis
Availability During Disaster Recovery Plan	Provide redundancy, diversity, or other means, in a disaster recovery plan to ensure service delivery continues in the event of a failure	Continue to deliver 99.995% uptime in the event of a Core or distribution layer failure; 99.99% uptime at the VAMC facility layer; 99.9% uptime at the remote locations
Failover Time	Failover to backup capability shall occur within 15 minutes of identification of a primary system failure.	100% of the time

Performance Objective	Performance Standards	Acceptable Performance Levels
Failover Notification	Inform VA PM of failover within 5 minutes of failover.	100% of the time.
Contract Deliverables	Provide deliverables to the appropriate Points of Contact in accordance with the schedule set forth in Schedule B	The Contractor shall provide all contract deliverables 100% on time
Operator Services	Operator consoles and connectivity shall be provided and must be available 24 hours a day, seven days a week, and 365 days a year	100% of the time
Voicemail Password Resets	Complete Individual Requests for voicemail password resets within 30 minutes	95% of the time
	Complete Individual Requests for voicemail password resets within 60 minutes	100% of the time
Software Change Requests	Complete Individual Requests for software changes within 1 business day	95% of the time
	Complete Individual Requests for software changes within 3 business days	100% of the time
Bulk Service Requests (e.g. workgroup moves)	Process bulk service requests within 10 business days.	100% of the time
Priority 1 and 2 Event notification	To the extent possible with in place systems, applications, and tools; have events, which result in an EVS PoC Priority 1 or 2 incident, generate an alert that is presented to the Contractor's EVS PoC Enterprise Helpdesk staff within 10 minutes of the event occurring.	100% of the time except when the event is prevented from being presented to the Contractor's EVS PoC Enterprise Helpdesk staff by a limitation or breakdown in government managed hardware, software, processes, procedures, or partners.
EVS PoC System Alert	Initiate response to EVS PoC system alerts in the network management system	95% of the time

Performance Objective	Performance Standards	Acceptable Performance Levels
Response Time	(NMS) within 5 minutes.	
	Initiate response to EVS PoC system alerts in the network management system (NMS) within 30 minutes.	100% of the time
Email Notification Response Time	Respond to email notifications of EVS PoC events within 30 minutes	95% of the time
	Respond to email notifications of EVS PoC events within 60 minutes	100% of the time
EVS PoC Incident Response Time	Respond to EVS PoC incidents of priority 1 and 2 within 5 minutes; of priority 3 within 1 hour; and of priority 4 within 1 business day	95% of the time
	Respond to EVS PoC incidents of priority 1 and 2 within 10 minutes; of priority 3 within 2 hours; and of priority 4 within 2 business days	100% of the time
EVS PoC Incident Resolution Time	Resolve EVS PoC incidents, caused by EVS PoC hardware or software, of Priority 1 within 2 hours; of Priority 2 within 4 hours; of Priority 3 within 8 hours; an of Priority 4 within 5 business days.	95% of the time measured on a monthly basis Does not apply to EVS PoC incidents caused by non-EVS PoC hardware, software, infrastructure, or services; e.g., LAN, WAN, PSTN, Power, HVAC.
Provide Incident Logs	Provide incident logs within eight hours or less of request	100% of the time measured on a monthly basis
Reporting of Network Intrusions and/or Data Breaches	Immediately report suspected or confirmed network intrusions and/or data breaches to the VA NSOC, EVS PoC Project Manager, and EVS PoC ISO	100% of the time
Helpdesk Speed of Answer	Helpdesk calls shall be answered within 18 seconds (three rings)	95% of the time
	Helpdesk calls shall be answered within	100% of the time

Performance Objective	Performance Standards	Acceptable Performance Levels
	42 seconds (seven rings)	
Helpdesk Voicemail Response Time	Return voicemail messages left for the EVS PoC Enterprise Helpdesk within 30 minutes.	95% of the time
	Return voicemail messages left for the EVS PoC Enterprise Helpdesk within 120 minutes.	100% of the time
EVS PoC Change Standards Compliance	Ensure that all EVS PoC changes are compliant with VA security and technical policies and standards; e.g., Assessment and Authorization, TRM, and CRISP.	100% of the time
EVS PoC Change Success	EVS PoC Changes are Successful	100% of the time
EVS PoC Change Completion Time	Ensure that EVS PoC changes are completed within the scheduled and approved change/maintenance window for each change.	95% of the time
Core Audit Records Storage	Allocate audit record storage capacity and configure auditing to prevent audit record storage capacity being exceeded for EVS PoC Core auditable events	100% of the time
COOP Support	Remotely implement and support EVS PoC systems and services, for use in COOP implementation, to be sustained for up to 30 days.	Within 12 hours of COOP Activation

The Government 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 manner. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. ***<VERIFY next statement and remove if not using the survey>*** A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.5 FACILITY/RESOURCE PROVISIONS

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

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

VA will provide access to VA specific systems/network as required for execution of the task via remote access technology (e.g. Citrix Access Gateway (CAG), site-to-site VPN, or VA Remote Access Security Compliance Update Environment (RESCUE)). This remote access will provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize Government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED Additional VA Requirements, Consolidated and ADDENDUM B - VA Information And Information System Security/Privacy Language.

6.6 GOVERNMENT FURNISHED PROPERTY

Contractor access to government IT systems shall be provided only to duly cleared contract personnel at the specified government facilities (see section 4.6 – Security and Addenda A and B, below) and via Citrix Access Gateway (CAG). Access to EVS PoC systems will not be available via the CAG. CAG will allow access only to ancillary VA systems such as e-mail and Lync. Government Furnished Equipment (GFE) shall be provided as necessary for EVS PoC Service Desk personnel to administer and maintain EVS PoC systems and utilize network management systems.

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

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

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for 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, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the Project Manager, 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), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

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

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this 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.

A2.1. 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): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

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

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

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

A3.1. Section 508 – Electronic and Information Technology (EIT) Standards

(Two standards listed below [§ 1194.31 Functional Performance Criteria and § 1194.41 Information, Documentation, and Support] always apply and should remain marked as "x". The requiring activity should un-mark any of the other remaining standards below that do not apply to this effort.)

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and

Information Technology (EIT). These standards are found in their entirety at: http://www.section508.gov and http://www.section508.gov/acquisition-regulations. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_x_ § 1194.25 Self contained, closed products
_x_ § 1194.26 Desktop and portable computers
_x_ § 1194.31 Functional Performance Criteria
_x_ § 1194.41 Information, Documentation, and Support

A3.2. Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

A3.3. Compatibility with Assistive Technology

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

A3.4. Representation of Conformance

In order to be considered eligible for award, offerors must submit the Government Product Accessibility Template (GPAT) to verify Section 508 conformance of their products and/or services. The GPAT will be incorporated into the resulting contract.

A3.5. Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include a final/updated GPAT and final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government

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

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment. Additional information concerning tools and resources can be found at http://www.section508.va.gov/section508/Resources.asp.

Deliverable:

A. Updated GPAT
B. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

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

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or 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.

A5.0 Confidentiality and Non-Disclosure

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

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

Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

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 Contracting Officer 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 Contracting Officer 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 Contracting Officer.
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:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.

b. Controlled access to system and security software and documentation.
c. Recording, monitoring, and control of passwords and privileges.
d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
h. Contractor does not require access to classified data.

8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.
9. VA Form 0752 shall be completed by all Contractor employees working on this 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.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 13514, “Federal Leadership in Environmental, Energy, and Economic Performance,” dated October 5, 2009; Executive Order 13423, “Strengthening Federal Environmental, Energy, and Transportation Management,” dated January 24, 2007; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, FEMP designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at www.femp.energy.gov/procurement. The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

If the acquisition is NOT Lowest Price Technically Acceptable (LPTA) please insert the following language into paragraph 3 above (in black text): "The acquisition of Silver or Gold EPEAT registered products is encouraged over Bronze EPEAT registered products".

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

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

(Addendum B must be tailored according to the requirements of the effort. Use the "Crosswalk" section of the "Flowchart and Guide, 6500.6 Appendix A" for assistance in determining the required sections to be included in the PWS. Instructions in blue text before each section is general guidance, for more specific guidance, please refer to the "Flowchart and Guide, 6500.6. Appendix A")

(Also, in Section B4, please complete the fill-in-the blank areas based upon the specific requirement for the current effort.)

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

B1. GENERAL

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

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

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

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

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract

personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

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

e. The Contractor or Subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor's employ. The Contracting Officer must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

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

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

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements

as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Contracting Officer within 30 days of termination of the contract.

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

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

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

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

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

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

10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of

competent jurisdiction, or (ii) with VA prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA contracting officer for response.

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

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

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

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

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC

configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

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

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

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

7. The Contractor/Subcontractor agrees to:

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

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

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

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

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

the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

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

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

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

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

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**,** based upon the severity of the incident.

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within the contract.

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

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

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

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

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

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies

must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

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

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

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

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

1) Vendor must accept the system without the drive;

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

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

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

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

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

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

B6. SECURITY INCIDENT INVESTIGATION

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

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

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

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

B7. LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.

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

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

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

a) date of occurrence;

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

3) Number of individuals affected or potentially affected;

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

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

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

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

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

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

10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and

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

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

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

B9. TRAINING

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

1) Successfully complete the *VA Privacy and Information Security Awareness and Rules of Behavior* course (TMS #10176) and complete this required privacy and security training annually; Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, Appendix D relating to access to VA information and information systems.

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

b. The Contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

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

Notes to the Contracting Officer

(This section to be removed from PWS before solicitation)

TYPE OF CONTRACT(S)

(Choose the type of contract that applies by selecting the checkbox, or, if a hybrid, select all that apply)

- ☐ Firm Fixed Price
- ☐ Cost Reimbursement
- ☐ Labor-Hour
- ☐ Time-and-Materials
- ☐ Other _____

SCHEDULE FOR DELIVERABLES

Note: Days used in the table below refer to calendar days unless otherwise stated. Deliverables with due dates falling on a weekend or holiday shall be submitted the following Government work day after the weekend or holiday.

Note: A ship to address must be provided for all hardware deliverables. Electronic submission of S/W or paper deliverables should be the norm unless otherwise stated. Email address(es) must be provided. Although email addresses are provided below for all PoC's, table must be clear as to who receives the deliverables.

Task	Deliverable ID	Deliverable Description
5.1.1	A	**Contractor Project Management Plan** Due within two weeks of contract award Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.2	A	**EVS PoC Sustainment Project Kickoff Meeting Agenda** Due within two weeks of contract award unless VA has extenuating circumstances preventing attendance Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.2	B	**EVS PoC Sustainment Project Kickoff Briefing** Due within two weeks of contract award Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.1.2	C	**EVS PoC Sustainment Project Kickoff Meeting Minutes** Due within two business days after Sustainment Kickoff Meeting Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3.1	A	**Weekly Status Call Agenda** Due within two business days of each Weekly Status Call Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3.1	B	**Weekly Status Call Minutes** Due within two business days of each Weekly Status Call Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3.1	C	**Weekly Status Report** Due weekly, beginning the first week after contract award Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.3.2	A	**Monthly Progress and Performance Report** Due by the 5th of each month. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.1.4	A	**Executive Leadership Briefing** Due 30 days after contract award, with a minimum of two briefings per month Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.2.1	A	**Phase-In Transition Plan** Due calendar 14 days after contract award Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.2.2	A	**Phase-Out Transition Plan** Due no later than calendar 60 days prior to the end of the contract POP Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.1	A	**EVS PoC Daily Operations Summary Report Template** Draft due 45 days after contract award; final due 14 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.1.1	B	**EVS PoC Daily Operations Summary Report** First report due within 7 days after the template has been finalized; updated report delivered on a daily basis thereafter Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.2	C	**EVS PoC Weekly Operations Report Template** Draft due 60 days after contract award; final template due 14 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.2	D	**EVS PoC Weekly Operations Report** First report due within 14 days after the template has been finalized; an updated report due on a weekly basis thereafter Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.3	E	**EVS PoC Monthly Operations Report Template** Draft due 75 days after contract award; final template due days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.3	F	**EVS PoC Monthly Operations Report** First report due within 30 days after the template has been finalized; due on or before the 10th day of each month Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.1.4	G	**EVS PoC Dashboard** Draft due 90 days after contract award; first EVS PoC Dashboard due 180 days after contract award. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.5	A	**EVS PoC Site Access Procedures Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.7	B	**EVS PoC Site Access Procedures** A draft due 30 days after the template has been finalized; initial document due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.2.1.4.3	C	**EVS PoC Enterprise Helpdesk Business Continuity Plan Template** A draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.4.3	D	**EVS PoC Enterprise Helpdesk Business Continuity Plan** Draft due 60 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.6	E	**EVS PoC Manufacturer Support Contract List Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.6	F	**EVS PoC Manufacturer Support Contract List** Draft due 30 days after the template has been finalized; initial due 300 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.6	G	**EVS PoC Manufacturer Support Contract Quarterly Report Template** Draft due 100 days after contract award; final due 35 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.6	H	**EVS PoC Manufacturer Support Contract Quarterly Report** Draft due 35 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA; subsequent reports due by the 10th day of each calendar quarter. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.1.6	I	**EVS PoC Manufacturer Support Contract Audit Report Template** Draft due 100 days after contract award; final due 35 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.2.1.6	J	**EVS PoC Manufacturer Support Contract Audit Report** Draft due 35 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA; subsequent reports shall be delivered by March 31st of each year Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.2	K	**EVS PoC Request Fulfillment Procedures Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.2	L	**EVS PoC Request Fulfillment Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.3	M	**EVS PoC Event Management Procedures Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.3	N	**EVS PoC Event Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.3	O	**EVS PoC Event Management Monthly Audit Report Template** Draft due 30 days after contract award; final due 15 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.3	P	**EVS PoC Event Management Monthly Audit Report** Initial report due 30 days after the template has been finalized; subsequent reports shall be delivered the 10th of each month. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.2.5	Q	**EVS PoC Incident Management Procedures** Draft due 120 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	R	**EVS PoC Incident Escalation and Notification Procedures Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	S	**EVS PoC Incident Escalation and Notification Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	T	**EVS PoC Incident Escalation and Notification Contacts Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	U	**EVS PoC Incident Escalation and Notification Contacts** Draft due 30 days after the template has been finalized; initial ldue 30 days after the Contractor has received comments from the VA; verify/audit the list annually each November, and publish an updated list by December 15th each year Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	V	**EVS PoC Supplier Service Level Agreements Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.5	W	**EVS PoC Supplier Service Level Agreements** Draft due 30 days after the template has been finalized; initial ldue 30 days after the Contractor has received comments from the VA; verify/audit the list annually each November, and publish an updated list by December 15th each year Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.2.7	X	**EVS PoC Problem Management Procedures Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.2.7	Y	**EVS PoC Problem Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.1	A	**EVS PoC System Administration Task Schedule Template** Draft due 180 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.1	B	**EVS PoC System Administration Task Schedule** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.1	C	**EVS PoC System Administration Task Log Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.1	D	**EVS PoC System Administration Task Procedures Template** Draft due 210 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.1	E	**EVS PoC System Administration Task Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.3.2	F	**EVS PoC Application Administration Task Schedule Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.2	G	**EVS PoC Application Administration Task Schedule** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.2	H	**EVS PoC Application Administration Task Procedures Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.2	I	**EVS PoC Application Administration Task Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.2	J	**EVS PoC Application Administration Task Log Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.3	K	**EVS PoC Storage Management Task Schedule Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.3	L	**EVS PoC Storage Management Task Schedule** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.3.3	M	**EVS PoC Storage Management Task Log Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.3	N	**EVS PoC Storage Management Task Procedures Template** Draft due 120 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.3	O	**EVS PoC Storage Management Task Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.4	P	**EVS PoC Connections and Integration Points List Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.3.4	Q	**EVS PoC Connections and Integration Points List** Draft due 30 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA. The Contractor shall audit the list annually Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.2	A	**EVS PoC Release Plan(s)** Due within 7 days after the release is deployed. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.2	B	**EVS PoC Release Evaluation Report(s)** Due within 14 days after a release is deployed Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.1	C	**EVS PoC Build Package Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.4.1	D	**EVS PoC Build Package(s)** Due as needed to stay compliant with CRISP, VA EA, and VA TRM Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.1	E	**EVS PoC Build Schedule Template** Draft due 120 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.1	F	**EVS PoC Build Schedule** Initial due 60 days after the template has been finalized Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.1	G	**EVS PoC Build Management Procedures Template** Draft due 210 days after contract award, final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.4.1	H	**EVS PoC Build Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	A	**EVS PoC Change Review Meeting Agenda Template** Draft due 15 days after contract award; final of each template due 15 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	B	**EVS PoC Change Review Meeting Agenda** Due prior to each meeting; publish after each meeting Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	C	**EVS PoC Change Review Meeting Minutes Template** Draft due 15 days after contract award; final of each template due 15 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.5.1	D	**EVS PoC Change Review Meeting Minutes** Due prior to each meeting; publish after each meeting Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	E	**EVS PoC Change Schedule Template** Draft due 15 days after contract award; final due 7 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	F	**EVS PoC Change Schedule** Initial due 10 days after the template has been finalized Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	G	**EVS PoC Change Management Procedures Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.1	H	**EVS PoC Change Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.2	I	**EVS PoC Maintenance Window List Template** Draft due 30 days after contract award; final due 15 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.2	J	**EVS PoC Maintenance Window List** Draft due 30 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.3	K	**EVS PoC Configuration Management Procedures Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.5.3	L	**EVS PoC Configuration Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.3	M	**EVS PoC Configuration Management Audit Report Template** Draft due 330 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.3	N	**EVS PoC Configuration Management Audit Report** Initial due 15th of option year one (1); subsequent reports shall be delivered March 15th each year thereafter Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.3	O	**EVS PoC Configuration Management Detail Report** Due within three business days upon request from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.4	P	**EVS PoC Asset Management Procedures Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.4	Q	**EVS PoC Asset Management Procedures** Draft due 90 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.4	R	**EVS PoC Asset Management Audit Report Template** Draft due 330 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.5.4	S	**EVS PoC Asset Management Audit Report** Initial due March 15th of option year one (1). Subsequent reports shall be delivered March 15th each year thereafter Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.5.4	T	**EVS PoC Asset Management Detail Report(s)** Due within three business days upon request from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.1	A	**EVS PoC Service Performance Plan(s)** As needed to prevent or remediate EVS PoC service performance issues Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.2	B	**EVS PoC Availability Management Procedures Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.2	C	**EVS PoC Availability Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.3	D	**EVS PoC Capacity Management Procedure Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.3	E	**EVS PoC Capacity Management Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.3	F	**EVS PoC Quarterly Capacity Plan Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.6.3	G	**EVS PoC Quarterly Capacity Plan** Draft due 60 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA. Subsequent capacity plans shall be delivered by the 15th day of each calendar quarter Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.7	A	**EVS PoC Security Management Task Schedule Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7	B	**EVS PoC Security Management Task Schedule** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7	C	**EVS PoC Security Management Task Log Template** Draft due 90 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7	D	**EVS PoC Security Management Task Procedures Template** Draft due 90 days after contract award; final procedures template shall be delivered 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7	E	**EVS PoC Security Management Task Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.1	F	**EVS PoC Access Management Procedures Template** Draft due 30 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.1	G	**EVS PoC Access Management Procedures** Draft due 30 days after the template has been finalized; final due shall be delivered 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.7.1	H	**EVS PoC Access Management Annual Audit Report Template** Draft due 30 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.1	I	**EVS PoC Access Management Annual Audit Report** Draft due January 10th of each calendar year; final report shall be delivered January 31st of each calendar year Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.1	J	**EVS PoC Access Management Remediation Report Template** Draft due 60 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.1	K	**EVS PoC Access Management Remediation Report** Draft due February 15th of each calendar year; final due each calendar year, 15 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.3	L	**EVS PoC Weekly Audit Record Report** Due on a weekly basis and report findings to VA in the EVS PoC Weekly Operations Report. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.7	M	**EVS PoC Security Incident Notification and Escalation List and Procedures Template** Draft due 30 days after contract award; final due 15 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.7	N	**EVS PoC Security Incident Notification and Escalation List and Procedures** Draft due 15 days after the template has been finalized; final document due 15 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.4	O	**EVS PoC Emergency Shutdown Procedures Template** Draft due 120 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.7.4	P	**EVS PoC Emergency Shutdown Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.1	Q	**EVS PoC Consolidated ISCP Performance Targets Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.1	R	**EVS PoC Consolidated ISCP Performance Targets** Draft due 30 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9	S	**EVS PoC Core ISCP** Due a minimum of one time annually Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.2	T	**EVS PoC ISCP Training Plan Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.2	U	**EVS PoC ISCP Training Plan** Draft due 30 days after the template has been finalized; initial due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.2	V	**EVS PoC ISCP Training Materials (compatible with TMS)** Draft TMS compatible EVS PoC ISCP training materials due 210 days after contract award; TMS compatible EVS PoC ISCP training materials due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	W	**EVS PoC ISCP Test Plan Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.3.7.9.3	X	**EVS PoC ISCP Test Plan** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	Y	**EVS PoC ISCP Test Report Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	Z	**EVS PoC ISCP Test Report** Due within 14 days after each exercise Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	AA	**EVS PoC ISCP Exercise Plan Template** Draft due 150 days after contract award; final due 30 days after the Contractor has received comments from the VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	BB	**EVS PoC ISCP Exercise Plan** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from the VA. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	CC	**EVS PoC ISCP Exercise Report Template** Draft due 150 days after contract award; report due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.3.7.9.3	DD	**EVS PoC ISCP Exercise Report** Due within 14 days after each exercise Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.3	A	**Voicemail Migration Plan for Ft. Harrison** Due within 60 days of exercise of option Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.4.3	B	**Voicemail Migration Plan for Charleston** Due within 60 days of exercise of option Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.3	C	**Voicemail Migration Plan for Tennessee Valley** Due within 60 days of exercise of option Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.4	A	**Site Design (Per Site/Location)** Due 30 days after exercise of this option Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.4	B	**As Built Site Design (Per Site/Location)** Due within 30 days of VA acceptance of installation Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.5	A	**System Migration to CVI for Ft. Harrison** Due within 60 days of exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.5	B	**System Migration to CVI for Charleston** Due within 60 days of exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.5	C	**System Migration to CVI for Tennessee Valley** Due within 60 days of exercise of option. Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.6	A	**IPv6 Design and Approach** Due anytime there is an IPv6 change Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.7.1	A	**VANTS Integration Design and Approach** Due anytime there is an VANTS change Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.4.7.2	A	**MS Lync Integration Design and Approach** Due anytime there is an Lync Integration change Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.7.3	A	**EVTN Integration Design and Approach** Due anytime there is an EVTN change Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.7.4	A	**Local Application Integration Design and Approach** Due anytime there is a change to a local third party application Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.7.5	A	**Unified Communication Integration Design and Approach** Due anytime there is an change to a Unified Communication Application Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.9	A	**EVS PoC Capacity Augmentation Cost Estimate** Due within 30 days of exercise of option, no more than once every 90 days Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.10	A	**EVS PoC Database Administration Task Schedule Template** Draft due 30 days after exercise of option; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.10	B	**EVS PoC Database Administration Task Schedule** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.10	C	**EVS PoC Database Administration Task Log Template** Draft due 30 days after exercise of option; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

Task	Deliverable ID	Deliverable Description
5.4.10	D	**EVS PoC Database Administration Task Procedures Template** Draft due 30 days after exercise of option; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
5.4.10	E	**EVS PoC Database Administration Task Procedures** Draft due 30 days after the template has been finalized; final due 30 days after the Contractor has received comments from VA Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
6.2.2	A	**Contractor Staff Roster** Due 3 days after contract award and updated throughout the PoP Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
A4.5	A	**Updated GPAT** Due 5 days after testing is completed Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination
A4.5	A	**Final Section 508 Compliance Test Results** Due 5 days after testing is completed Electronic submission to: VA PM, COR, CO. Inspection: destination Acceptance: destination

(Note: If a deliverable is requested in draft, and then final submission-the deliverable line item is complete, no further update can be requested. Continued reporting should be a separate line item.)

INSPECTION and ACCEPTANCE / Free on board (FOB) for Shipped Deliverables

(NOTE: (Deliverables table reflects the Inspection and Acceptance) Include additional information if other than standard inspection and acceptance is required. If any hardware/software is being purchased (incidental to the service being performed), state the acceptance criteria and provide Shipping Address /Mark For requirements.

Inspection and acceptance shall be at ***<origin OR destination>*** and FOB shall be ***<origin OR destination OR indicate N/A > (N/A if the deliverable is a service item)*** Ship to address is: ***<enter all Address/Mark For requirements>***.

Special Shipping Instructions:

Prior to shipping, Contractor shall notify Site PoCs, by phone followed by email, of all incoming deliveries including line-by-line details for review of requirements. Contractor shall not make any changes to the delivery schedule at the request of Site PoC.

Contractors shall coordinate deliveries with Site PoCs before shipment of <hardware> hardware to ensure sites have adequate storage space. All shipments, either single or multiple container deliveries, will bear the VA Purchase Order number on external shipping labels and associated manifests or packing lists. In the case of multiple container deliveries, a statement readable near the VA PO number shall indicate total number of containers for the complete shipment (i.e. “Package 1 of 2”), clearly readable on manifests and external shipping labels.

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (i.e., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Total number of Containers: Package ___ of ___. (i.e., Package 1 of 3)

NOTE: VA XXX Initiative ***(if applicable)***

POINTS OF CONTACT
(Identify PoCs for this effort for distribution of deliverables)

VA Program Manager:
Name: Willie Wilson
Address:
Voice:
Email:

Contracting Officer’s Representative:
Name: DeWayne Porter
Address:
Voice:
Email:

Contracting Officer:
Name: Debbie Clayton
Address:
Voice:
Email:

ADDITIONAL ITEMS

SPECIAL INSTRUCTIONS/REMARKS

(Include delivery instructions; required Delivery dates in terms of number of days after receipt of order (ARO) or days after contract (DAC); where is equipment going; mark for requirements (name of a person)/receiving contact; prior year PO#s, proposed payment provisions; Government furnished property; suggested contract clauses; other valuable information, etc., as applicable). Provide additional documentation if needed.

SPECIAL CLAUSES, ETC. TO BE INCLUDED IN THE SOLICITATION

(Choose Special Clause(s), etc., if applicable, by selecting the checkbox and modifying as necessary)

☐ Transition clause required?
(Insert FAR clause, Continuity of Services, FAR 52.237-3)
☐ Intellectual Property/Technical Data Rights Clause required?
☐ OCI Clause required?
☐ Government Furnished Material/Equipment: CO should add a special clause to the contract citing the Title of the material/equipment, Identifier (Serial Number), Quantity, Purpose, and Date required by Contractor.
☐ BAA required?
If the answer to Question 4 of the Security Checklist is a "yes" and the Contractor will provide a service, function, or activity to the Veterans Health Administration (VHA) or on behalf of VHA, then it must be determined if protected health information is disclosed or accessed and if a BAA is required. The "Decision Tree for Business Associate Agreements" should be used by the requiring activity (with help from their Privacy Officer if needed) to determine if a BAA is required, see VHA Handbook 1605.05, Business Associate Agreements, Appendix A, (http://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3027). If it is determined that a BAA is required, the CO must, in eCMS, insert the VHA clause 1605.05 into Section D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS of the solicitation. This can be accomplished by performing the following in eCMS:

1. Insert the 1605.05 clause through the Clause Library (or by answering "Yes, access to PHI is necessary and a BAA is required," to the Dialog Session question that asks, "Will the contractor require access to Protected Health Information to perform the functions or services required in this acquisition?")
2. After inserting the clause, double-click on the clause and use the "Fill-in" field in the "Scope" section to add a description of the service(s) being performed.
3. In the MS Word version of your solicitation, manually input "Contractor" throughout the document where it has been blanked out. The embedded file below shows the locations of the "blanks" (showing codes from eCMS

in red instead of “blanks”) to assist you in adding the missing information properly. The eCMS VHA Clause 1605.05 text is the BAA itself and needs to be seen by the bidders if a BAA is required. Note: The actual Contractor’s Name will automatically populate in the appropriate sections of the BAA clause from the Data Values upon creation of the award document.

VHA 1605.05
BUSINESS ASSOCIAT

☐ Other _____
☐ Other _____

FOR TAC USE ONLY---SECURITY RELATED GUIDANCE

☒ **(Always Checked for Services)** Addendum B Security Requirement guidance to CO within Addendum B, Section B9 Training, Para. a) Sub Para. d,

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

☒ **(Always Checked for Services)** Contractor Rules of Behavior-Appendix D in Handbook 6500.6 – (CO to add to solicitation, CO to ensure Contractor signs document)

ADDENDUM C – EVS POC LOCATION ADDRESSES

VA CENTRAL OFFICE

The Contract shall, when required, attend meetings at the VA Central Office (VACO) at 810 Vermont Ave NW

Washington, D.C., or nearby locations designated by the CO, COR, or their designee(s).

VA CORE SITES

Core locations provide the intelligence, call routing and enterprise architecture for VA's EVS PoC infrastructure using a nationwide dial plan. The Core shall provide for EVS PoC site inter-connectivity to allow for on-net calling. The current cores at Hines, IL and Austin, TX also provide voicemail storage and retrieval for the EVS PoC sites which shall be moved down to the primary sites.

Core Locations – Chicago, IL and Austin, TX

Facility Type	Facility Name	Facility Address
Core	Austin Data Center	1615 Woodward Street, Austin, TX 78772
Core	Hines Data Center	5000 South 5th Ave, Building 215, Hines, IL 60141

SUPPORT SITES

Facility Type	Facility Name	Facility Address
Service/Technical Support Center	EVS Helpdesk	Falling Waters, WV

PRIMARY SITES

VA Montana Health Care System

The primary PoC location for the VA Montana Health Care system is the Fort Harrison VA Medical Center in Fort Harrison, MT, and includes approximately 3,000 general users and approximately 350 users that require more advanced attendant and call routing features. This PoC location does not service or house any of VA's major call center locations; however, it does host a local call center. The Ft. Harrison VBA Claims Center does not require EVS PoC and will retain its existing voice system with only the reconnecting of trunks to the Ft. Harrison VAMC system to ensure local dialing capability remains intact. This PoC location is comprised of a VAMC and remote

facilities such as Community Based Outpatient Clinics (CBOCs) and Veteran Centers (Vet Centers).

Facility Type	Facility Name	Facility Address
Primary Location		
VAMC	VA Medical Center and Ambulatory Care Clinic	3687 Veterans Drive, Fort Harrison, MT 59636
Medical Centers and Remote Locations		
CBOC	Bozeman VA Community Based Outpatient Clinic	300 N. Wilson, Suite 703G, Bozeman, MT 59715
CBOC	Anaconda VA Community Based Outpatient Clinic	118 East 7th St., Suite 2A, Anaconda, MT 59711
OPC	Hamilton Primary Care Telehealth Outreach Clinic	299 Fairgrounds Suite A, Hamilton, MT 59840
Vet Center	Missoula Vet Center	500 N. Higgins Avenue, Suite 202, Missoula MT 59802
CBOC	Missoula VA Community Based Outpatient Clinic	2687 Palmer Street, Suite C, Missoula, MT 59808
Vet Center	Kalispell Vet Center	690 North Meridian Road, Suite 101, Kalispell MT 59901
CBOC	Kalispell VA Community Based Outpatient Clinic	31 Three Mile Dr. Ste. 102, Kalispell, MT 59901
Pharmacy	Pharmacy VA Remote Pharmacy	400 Veterans Drive Columbia Falls, MT 59912
CBOC	Cut Bank VA Community Based Outpatient Clinic	#8 2nd Ave SE, Cut Bank, MT 59427
CBOC	Havre VA Community Based Outreach Clinic	130 13th Street, Suite 1, Havre, MT 59501
CBOC	Glasgow VA Community Based Outpatient Clinic	630 Second Ave. South, Suite A, Glasgow, MT 59230
OPC	Plentywood Primary Care Telehealth Outreach Clinic	440 West Laurel Avenue, Plentywood, MT 59254
CBOC	Glendive VA Community Based Outpatient Clinic	2000 Montana Ave., Glendive, MT 59330
CBOC	Miles City VA Community Based Outreach Clinic/ Nursing Home	210 S. Winchester, Miles City, MT 59301
Lab	Billings Mental Health/C&P/Lab	2345 King Avenue West Billings, MT 59102
Vet Center	Billings Vet Center	2795 Enterprise Ave., Suite 1, Billings MT 59102
CBOC	Billings VA Community Based Outpatient Clinic	1775 Spring Creek Lane, Billings, MT 59102
CBOC	Lewistown VA Community Based Outpatient Clinic	629 NE Main Street. Suite 1, Lewistown, MT 59457
CBOC	Great Falls VA Community Based Outpatient Clinic	1417-9th Street South, Suite 200 and 300, Great Falls, MT 59405
Vet Center	Great Falls Vet Center	615 2nd Avenue North, Great Falls MT 59401
Admin	Network Authorization Office and Helena Contracting Office	2905 North Montana Suite 108 Helena, MT 59601
Admin	Helena NARU – 3rd Party Claims	40 W 14th Street, Third Floor, Helena, MT 59601
Lab	Sleep Lab	2271 Deerfield Ln, Helena, MT 59601

Ralph H. Johnson VA Medical Center, Charleston, SC

The primary PoC location in Charleston, SC includes approximately 3,000 general users and approximately 30 users that require more advanced attendant and call routing features. This PoC location does not service or house any of VA's major call center locations; however, it does host a local call center. This PoC location is comprised of one VA Medical Center (VAMC) and remote facilities such as Community Based Outpatient Clinics (CBOCs) and Veteran Centers (Vet Centers).

Facility Type	Facility Name	Facility Address
Primary Location		
VAMC	Ralph H. Johnson VA Medical Center	109 Bee Street, Charleston, SC 29401
Medical Centers and Remote Locations		
CBOC	James Island Annex	325 Folly Road, Charleston, SC 29412
Call Center	Montague Call Center	3355 West Montague Avenue, North Charleston , SC 29418
Vet Center	Charleston Vet Center	3625 West Montague Avenue, North Charleston , SC 29418
Warehouse	Warehouse	1001 Trident St, North Charleston, SC 29406
CBOC	Trident Clinic	9237 University Blvd, North Charleston , SC 29418
CBOC and OPCs	Goose Creek Primary Care Clinic, DOD Joint Optometry, and VBA Comp. & Pension	2418 NNPTC Circle, Goose Creek, SC 29445
OPCs	Myrtle Beach Primary Care and Mental Health Services and Myrtle Beach Clinic	3381 Phillis Blvd., Myrtle Beach, SC 29577
Vet Center	Myrtle Beach Vet Center	2024 Corporate Centre Dr., Myrtle Beach, SC 29577
OPC	Conway Home Based Primary Care	914 Norman Alley, Conway , SC 29526
CBOC	Beaufort Clinic	1 Pinckney Boulevard, Beaufort, SC 29902
CBOC	Savannah Clinic	325 West Montgomery Crossroad, Savannah, GA 31406
Vet Center	Savannah Vet Center	321 Commercial Dr., Savannah, GA 31406
CBOC	Hinesville Clinic	500 East Oglethorpe Highway, Hinesville, GA 31313

Tennessee Valley Healthcare System

The two primary PoC locations in Tennessee Valley Healthcare System (TVHS) are in Nashville and Murfreesboro (connected by tie-lines) and its remote locations with approximately 4,365 general users and approximately 250 users that require more advanced attendant and call routing features. The locations within this PoC do not service or house any of VA's major call center locations; however, it does house a local call center. The PoC locations are comprised of two primary locations at the VAMCs and remote facilities such as CBOCs and Vet Centers. The VBA Office in Nashville

requires up to ten phones with basic voice services to serve as EVS PoC test phones and does not require a full replacement of their existing system. The EVS PoC test phones may not leverage the existing VBA voice system to perform EVS PoC functions.

Facility Type	Facility Name	Facility Address
Primary Location		
VAMC	Nashville Campus	1310 24th Avenue South, Nashville, TN 37212
VAMC	Alvin C. York Campus	3400 Lebanon Pike, Murfreesboro, TN 37129
Medical Centers and Remote Locations		
Admin	VISN 9: VA Mid South Healthcare Network	1801 West End Ave., Suite 600, Nashville TN 37203
Vet Center	Nashville Vet Center	1420 Donelson Pike Suite A-5, Nashville TN 37217
OPCs	Nashville (Charlotte Avenue) Outpatient Clinic and Women Veterans Healthcare Center (Nashville)	1919 Charlotte Avenue, Nashville, TN 37203
CBOC	Meharry (Nashville General) Outpatient Clinic	1818 Albion Street, Nashville, TN 3720
OPC	Clarksville Dental Clinic	2291 Dalton Drive, Suite F., Clarksville, TN 37043
CBOC	Clarksville Community Based Outpatient Clinic	1832 Memorial Dr., Clarksville, TN 37043
OPC	Athens Outreach Clinic	1320 Decatur Pike, Athens, TN 37303
Vet Center	Chattanooga Vet Center	951 Eastgate Loop Road Bldg. 5700 - Suite 300, Chattanooga TN 37411
CBOC	Chattanooga Community Based Outpatient Clinic	6098 Debra Rd Suite 5200 Bldg. 6200, Chattanooga, TN 37411
CBOC	McMinnville Community Based Outpatient Clinic	1014 S. Chancery Street, McMinnville, TN 37110
Admin & NCA Office	Stonegate NCA and VISN 9 Contracting Office	1639 Medical Center Pkwy, Suite 400, Murfreesboro, TN 37129
CMOP	Consolidated Mail Order Pharmacy	5171 Sam Jared Dr., Murfreesboro, TN 37130
IRDC	Informatics Research and Design Center	2187 West End Ave, Ste. 200, Nashville, TN 37203

ADDENDUM D – EVS POC TECHNICAL REQUIREMENTS

The Contractor shall provide, operate, and manage the Enterprise Voice System (EVS PoC) Proof of Concept (PoC) solution that meets and/or exceeds the requirements set forth in the following sections. The EVS PoC solution shall be and operated to provide enterprise calling, voicemail services, regional inter-site calling, and site-level EVS PoC survivability capability.

D.1.0 EVS POC SERVICE LEVEL AGREEMENT (SLA)

The Contractor shall ensure that its services shall conform to the following Service Level Agreement (SLA) parameters. All references to “Service Level Agreement” or “SLA” in this PWS shall include the requirements set forth in Section 6.4.

D.1.1 NSD PRIORITY MATRIX

The VA incident priorities defined in the table below, are used to measure Contractor performance of Incident Handling in Section 5.3.2.6.

Table D.1 - NSD Incident Priority Matrix

IMPACT	URGENCY 1	URGENCY 2	URGENCY 3	URGENCY 4	PRIORITY
1	1	1	2	3	
2	1	2	3	3	
3	2	2	3	4	
4	3	3	4	4	

IMPACT	Business
Level 1 – Critical	VA Wide
Level 2 – Serious	Regional/CDCO
Level 3 – Moderate	VISN/Station
Level 4 – Minimal	Local/ Individual

Notification Process	
	CIO/RDP/VHA/VBA Mgmt/CDCO Mgmt
	RDP/VHA Mgmt/CDCO Mgmt
	CDCO Mgmt
	No Notification

URGENCY	Level
Level 1 – Critical	Production System Unavailable
Level 2 – Serious	Production System Delayed (Potential Impact on Business Function)
Level 3 – Moderate	Production/PreProd/Development – System not working within design specification (Available – No Business Impact)
Level 4 – Minimal	Production/PreProd/Development – Request for Service (No Business Impact)

PRIORITY	Time to Repair Goal
1	0-2 hour window
2	2-4 hour window
3	4-8 hour window
4	>8 hour window

D.1.1.1 MANUFACTURER SUPPORT CONTRACT RESPONSE TIME.

The Contractor shall ensure all manufacturer supportable EVS PoC Core configuration items; e.g., hardware and software; are under a manufacturer support contract per the requirements listed in tables D.1 and D.2 below.

Table D.2 - Cisco Hardware and Software Manufacturer Support Requirements

LOCATION TYPE	WARRANTY	TELEPHONE	S/W	H/W	TECHNICIAN	RESPPONSE TIME			
	BASE WARRANTY	TELEPHONE SUPPORT (24x7)	FREE UPDATES	ADVANCE REPLACEMENT	ONSITE TECHNICIAN	NEXT BUISNESS DAY	4 BUSINESS HOURS	4 HOURS (24x7)	2 HOURS (24x7)
Core Layer Component	1 YR	Yes	Yes	Yes	Yes		X		
Local Layer Component (VAMC/Primary Site, and Remote/Secondary Site	1 YR	Yes	Yes	Yes	No		X		
Endpoints	1 YR	Yes	Yes	No	No	N/A	N/A	N/A	N/A
Spare Parts	1 YR	Yes	Yes	Yes	Yes		X		

Table D.3 - Other Manufacturer Software Support Requirements

CI Type	WARRANTY	TELEPHONE	SOFTWARE
	BASE WARRANTY	TELEPHONE SUPPORT (24x7)	FREE PATCHES
Microsoft (Win 2012 Server)	1 YR	Yes	Yes
VMware (VSphere Enterprise Plus)	1 YR	Yes	Yes
South River Technologies (Titan – SFTP)	1 YR	Yes	Yes
ScienceLogic (NMS system)	1 YR	Yes	Yes

D.1.2 SYSTEM PERFORMANCE, MONITORING, AND REPORTING

The Contractor shall ensure the following:

a. **SLA Definition:** The Contractor shall monitor the underlying infrastructure which defines EVS PoC. The Contractor shall utilize VA's service quality management tools to proactively detect and mitigate service quality degradation of Voice over Internet Protocol (VoIP) traffic and automatically report adverse events. The Contractor shall not be provided Simple Network Management Protocol (SNMP) access to any non-EVS PoC VA devices

b. **How Measured:** Once the VA PM and the Contractor have agreed to the acceptable performance levels and the reporting mechanism, the Contractor shall conduct performance measurements and report the findings monthly in the weekly and monthly operations reports.

c. **Event Escalation:** If in the execution of the weekly and monthly review, the Contractor finds the performance levels have fallen below the agreed to acceptable levels of call quality such as latency, jitter, the Contractor shall notify the VA PM and conduct a root cause analyses (RCA). The Contractor shall provide the RCA findings, a POA&M, and schedule to resolve the issues to the VA PM within five (5) business days of detection.

d. The EVS PoC Contractor shall proactively monitor the metrics defined below. The Contractor shall utilize VA's existing monitoring tools.

1. **Server Metrics**: CPU, Memory, Processes, Disk, Services, Network Services
2. **Call Metrics:** Voice Quality, Disconnect Cause, Call Categories, Latency Metrics, Packet Loss Metrics, Call Jitter, Call MOS, Active Call MOS, Call Status, Number of Incoming Calls, Number of Outgoing calls, Number of Calls to PSTN, Number of Office-to-Office Calls
3. **Phone Metrics:** Phone Status,
4. **Gateway Metrics:** Channel Availability, Utilization, Interface Status, Port Utilization
5. **Route Pattern Metrics:** Route Pattern Status, Route List/Group Status, Member Endpoints
6. **Media Server Metrics:** Conference Bridge, Transcoder, Music on Hold, Media Termination Points
7. **Trunk Metrics:** Utilization, Gatekeeper Registration Status
8. **TelePresence Metrics:** Peripheral Status, Call Quality Statistics
9. **Voicemail Metrics:** Service Availability, Voice Mail Port Usage, Unity Subscriber Numbers, Exchange Service Status, Mailbox Sizing and Utilization, Voicemail Time Used Percentage, Voicemail Available Storage Space, Voicemail Capacity, Orphaned Mailboxes
10. **Dial Peer Metrics:** Dial Peer Type, Destination Pattern, Successful Calls, Calls Refused, Calls Failed, Cause of Failure

D.1.3 AVAILABILITY

Availability is the measure of overall access to EVS PoC services and “uptime”, or reliability of the EVS PoC voice system infrastructure, to deliver the required services. The EVS PoC availability shall be:

- 99.9% - VA secondary facility services
- 99.99% - VA primary facility and distribution (if applicable) infrastructure
- 99.995% - Contractor Core Infrastructure

a. The availability of EVS PoC and VA local functions for a given month shall be calculated according to the formula below. EVS PoC and functions shall, subject to the exceptions listed below, be available for a percentage of each calendar month equal to the Service Level Commitment as specifically set forth in the SLA.

b. For purposes of this calculation, the solution will be deemed unavailable for any downtime or outages experienced by the end user. The Contractor’s reports, records and data shall be the sole basis for all SLA calculations and determinations, provided that VA may audit the Contractor’s records and data for the purpose of determining the accuracy of SLA calculations and determinations in accordance with the appropriate section of the SLA.

c. Unscheduled outages on redundant backup systems will not be included in the SLA calculation as long as it is not user service affecting and no current traffic is being routed through the redundant system.

d. The availability of EVS PoC and VA functions for a given month shall be calculated according to the following formula (referred to herein as the "Availability"):

   Total minutes in the month = TMM

   Total minutes in month unavailable = TMU

   Availability = ((TMM - TMU)/TMM) x 100

   The Percentage of Availability shall be calculated as the total number of minutes in the reporting period, less minutes of approved scheduled downtime (TMM); minus the minutes of downtime as a result of down or degraded services (TMU); divided by the total number of minutes in the reporting period (TMM); multiplied by 100,

   For example:

   Given 43,200 Total minutes in the month (24 hours x 60 minutes x 30 days = 43,200 minutes) and experiencing 120 total minutes in month unavailable, the formula would reflect the following:

   ((43,200 – 120) 43,200) x 100 = 99.72% Availability

D.1.4 NETWORK, LINK, AND INFRASTRUCTURE AVAILABILITY

The Contractor shall ensure the following network, link, and infrastructure availability:

a. Capacity and the management of congestion and blocked calls shall be considered part of network availability. Any external Session Initiation Protocol (SIP) trunking introduced shall be required to terminate at one of the VA Trusted Internet Connection (TIC) Gateways. VA will arrange gateway access rights at the co-location site.

b. EVS PoC services shall be available, whether it is during abnormal system operation or system upgrade regardless of hardware, software or user fault. Upon identification of a primary system failure, failover to a backup capability shall occur within 15 minutes of initial failure. The Contractor shall inform the VA PM within five (5) minutes of a failover.

c. The Contractor shall calculate EVS PoC Unavailability for each calendar month and include the results in the Monthly Progress and Performance Report. "Unavailability" consists of the time that EVS PoC was not available to VA in excess of the applicable availability metric.

d. Calculation of Unavailability shall not include any time EVS PoC is unavailable due to scheduled maintenance. The Contractor shall inform VA of what level of service degradation will be in place during the scheduled service window. The VA PM must approve the service window prior to scheduled maintenance taking place. The Contractor shall notify the VA PM within forty-eight (48) hours of unscheduled maintenance (unscheduled maintenance is defined as unplanned

maintenance that has not been scheduled and uncoordinated/advised with VA), not to exceed a four (4) hour period between Midnight and 4am local time once per calendar month. Scheduled maintenance requires 30 day's notification. Because these are medical facilities, it is critical that any scheduled maintenance be coordinated and managed in such a way that the facility retains voice service (defined as the ability to place and receive calls) at all times. Maintenance will be coordinated on a site by site basis to have minimal impact on Veteran services and patient care.

e. When adding capacity to EVS PoC, the Contractor shall ensure an additional 15 percent per annum of network and station capacity.

f. When a single LAN port is to be used for both the VoIP phone and PC data connection, the PC will plug into the built-in switch port of the IP phone. The Contractor shall ensure appropriate security is in place and VA will determine which IP phones; e.g., public access IP phones, lobby phones, courtesy phones; will have their switch ports disabled to prevent unauthorized access into the VA LAN

D.1.5 EFFECTIVE DATE

The SLAs shall start being measured on the start date of the contract.

D.2.0 USER PROFILES

The Contractor shall maintain configurations and telephones that conform to the following user types:

USER PROFILE & TELEPHONE CONFIGURATIONS										
	PUBLIC	PATIENT	GENERAL USER	CONTACT CENTER	CLINICIAN	ADMINISTRATIVE	OPERATOR	RECEPTIONIST	MANAGER	EXECUTIVE
Basic Features										
# of Physical Line Appearances	1	1	2	3	4	*	*	*	4	4
LCD Screen			●	●	●	●	●	●	●	●
Transfer			●	●	●	●	●	●	●	●
Hold			●	●	●	●	●	●	●	●
Basic Conference			●	●	●	●	●	●	●	●
Call Forwarding			●		●	●	●	●	●	●
Voicemail			●	●	●	●	●	●	●	●
Enhanced Features										
Enhanced Conferencing					●	●	●	●	●	●
Shared Line					●	●	●	●	●	●
Intercom					●	●	●	●	●	●
Extension Mobility			●		●	●		●	●	●
Agent Login/Logout				●						

AUX Code				●						
Acct Code		●	●		●	●	●	●	●	●
Call Park / Pickup /			●		●	●	●	●	●	●
Find / Follow Me			●		●				●	●
Paging					●	●	●	●	●	●
Calling Privileges										
Internal	●	●	●	●	●	●	●	●	●	●
Emergency	●	●	●	●	●	●	●	●	●	●
Local		●	●	●	●	●	●	●	●	●
Long Distance			●	●	●	●	●		●	●
International					●	●			●	●

Enhanced conferencing refers to the ability to conference on more than two additional parties in addition to originator on a conference call.

* The Contractor shall identify the required telephone line count required for each administrative, operator, and receptionist position at each location. The line count for administrative, operator, and receptionist positions is expected to be 6 or greater, and may require the use of one or more “side cars.” The Contractor shall provide a telephone that meets the line-count need for each administrative, operator, and receptionist position at each location.

D.3.0 OPERATOR AND E911 SERVICES

The Contractor shall maintain E911 services for every site and remote location and provide a description in the design approach of how their EVS PoC solution delivers E911 capabilities and complies with all applicable local and FCC regulatory requirements including Local Number Portability (LNP), directory assistance, and emergency services (911 or E911) requirements to identify the location of an originating station and route them to the appropriate Public Safety Answering Point (PSAP). Additionally, the Contractor shall describe any additional integration or equipment that is required to achieve this capability. Every telephone unit shall be capable of dialing and reaching an outside E911 operator.

The VAMC operators have a requirement that emergency calls display caller information (i.e. location, extension#); this feature is currently not available. This is critical to the primary location and shall be included as a function of EVS PoC. This capability is unique to the VAMC and does not apply to the remote locations.

Operators in VA facilities must be able to handle large quantities of calls with a single device. Operator consoles and connectivity shall be provided as a part of the solution. It must be available 24 hours a day, seven (7) days a week, and three 365 days a year. Users shall not receive a busy signal when calling operator services.

The Operator services function shall provide for:

a. Operator availability to assist users, including TDD/TTY users, encountering dialing difficulties when contacting VA. The operator shall have the ability to remain on the line until the call has been connected.

b. Where not identified as a specific auto-connect call, provide a hot-dial or direct-dial capability on phones such as hallway and elevator phones that connect directly to an operator, so that an internal emergency call can be routed appropriately; e.g., 911 or Code Blue.

D.4.0 EMERGENCY RESPONSE SERVICES REQUIREMENTS

The Contractor shall provide as part of EVS PoC, the continued ability to integrate and interoperate with IP and/or analog based devices such as High Frequency (HF) / Very High Frequency (VHF) radios, cellular telephones and wireless (Wi-Fi) enabled smartphones. This includes flexibility to operate in a limited capacity (i.e. basic voice service) in the event there is a loss of connectivity to the PSTN and EVS PoC core infrastructure given a catastrophic event, but shall allow disparate devices to communicate with one another (e.g. Land Mobile Radio (LMR) handheld radio to call a desk phone) in the locally affected area until full restoration of services is achieved.

D.5.0 HOTLINES

The Contractor shall provide the ability to perform a direct connection between two devices upon initiation of a call consistent with the current environments. This capability shall be provided at existing sites to include elevators, operating room, parking lots, boiler rooms, door entrances, and locked mental health wards. A hotline can automatically connect to any extension, not only to attendant positions and are private line auto ring downs.

D.7.0 CODEC AND PROTOCOL SUPPORT

The Contractor shall deliver a solution capable of supporting all of the following codecs and protocols:

1. G.729 Codec - VA requires the Contractor to provide a compressed codec, G.729, as part of their site connectivity back to their point of service to ensure that the additional traffic presented by EVS PoC does not require larger circuits than already in place, e.g., T1's. Not meeting this requirement could potentially overload the existing infrastructure connections and prove detrimental to the VA infrastructure by introducing unwanted latency or excessive traffic.
2. Session Initiation Protocol (SIP)
3. H.323
4. Media Gateway Control Protocol (MGCP)
5. G.711 – For use with TTY/TDD devices
6. 802.1x – Site will utilize Cisco ACS for 802.1x authentication and x.509 certificates will be provided by VA.

D.8.0 AUTOMATIC CALL DISTRIBUTION (ACD) AND INTERACTIVE VOICE RESPONSE (IVR) CAPABILITIES

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide the ACD and IVR capabilities in the table below. The Contractor shall propose solutions to reporting requirements, providing VA with the ability to generate ad hoc and real-time ACD reports.

Identifier	EVS PoC ACD Feature
1.0	Provide the ability for calls to be distributed to call agents via EVS PoC telephony
1.1	Provide the ability to integrate the ACD information with a workforce management (WFM) solution
1.2	Provide the ability for calls to be routed to a specific group of users
1.3	Provide the ability for call agents to receive incoming calls in order of their arrival
1.4	Provide music on hold and the ability to integrate at a minimum of four scripts
1.5	Provide the ability for administrator/supervisor to log phones/agent out of hunt groups
1.6	Provide the ability for staff to log into any phone and receive their personal and queue phone calls
1.7	Provide the ability to distribute calls to no less than 30 agents
1.8	Provide the ability to distribute calls to no less than 30 groups
1.9	Provide the ability to distribute calls to support different hours of operation
1.10	Provide the ability for the call agent to designate status as available to take a call.
1.11	Provide the ability for the call agent to designate when he/she is not available.
1.12	When an agent is available, provide the ability for the waiting call agent to be connected to the incoming call
1.13	Automatically present the next call to the call agent without requiring any action by the call agent (auto-enter)
1.14	If an agent is not available within a prescribed interval, provide the ability for all unanswered calls to be placed in the call-waiting queue and connected to delay announcements at pre-set time intervals
1.15	If a routed call is not answered within a specified period of time, provide the ability to return the call to the priority queue
1.16	Provide the ability to route the caller from an automated recording (exit point) to an agent
1.17	Provide the ability for the caller to hear announcements that provide an estimate on the time remaining before an agent will be available based on an ongoing dynamic sampling of relevant data for each established queue or group such as, average speed of answer, number of available agents
1.18	Provide the ability to create customized announcements for the caller to hear while waiting for an agent
1.19	Provide the ability to distribute incoming calls on a First In First Out (FIFO) basis
1.20	Provide the ability to distribute phone calls from a single telephone number to a

Identifier	EVS PoC ACD Feature
	group of telephones (hunt group)
1.21	Provide the ability to track/identify calls that have been auto forwarded
1.22	Provide the ability for the announcements to not influence the placement of a call in the queue
1.23	Provide the ability for the queue to always be served sequentially based on the time in queue and/or skill
1.24	Provide customizable call handling functionality based upon skill-based routing and longest call waiting
1.25	Provide the ability for the next call in queue to be distributed to the agent who has been idle longest
1.26	Provide the ability for a call to be moved to another agent within the same queue
1.27	Provide the ability for a call to be moved to another queue if one queue has too many calls
1.28	Provide the ability for a call surge capacity via IVR/ACD routing functionalities to include overflow capabilities to 3rd party sites
1.29	Provide the ability to allow an agent to answer multiple queues
1.30	Provide the ability for an administrator/supervisor to prioritize groups of callers in the queue
1.31	Provide skill prioritization functionality by agent (e.g., when an agent is available and two there are two calls waiting, the skill set (queue) with the highest priority for the agent will be answered first rather than the longest call waiting)
1.32	Provide the ability for administrator/supervisor to adjust the weighting factor for agents to receive calls
1.33	Provide IVR availability 24/7/365
1.34	After an agent completes the call or transfer function, provides the ability for the call agent to answer another incoming call. Note: a completed call includes wrap-up time
1.35	Provide the ability for the administrator/supervisor to manually force a call agent to go back to available or unavailable
1.36	Provide the ability to configure time post call to be used as call wrap-up
1.37	Provide the ability for the administrator/supervisor to schedule time when agents are not available
1.38	Provide the ability for the administrator/supervisor to schedule or mark call agents as available when the scheduled time off has completed
1.39	Provide the ability for the call agent to receive an alert when the time off period has been exceeded
1.40	Provide the ability for the administrator to associate a specific group of lines or line groups with a designated group of agents who have specific skills (for example interpreter)
2.0	Provide the ability for the administrator/supervisor to configure the following routing capabilities:
2.1	Number of queues

Identifier	EVS PoC ACD Feature
2.2	Queue announcements
2.3	Skill-based routing to specific agents or groups
2.4	Provide the ability to amend the list of skills used to route calls to agents (skills include: Client, Supervisor, Manager, Administrator/Technician)
2.5	Amount of time in queue before an overflow is determined
2.6	Number of calls in a queue before an overflow situation is determined
2.7	Modification of routing by date and time
2.8	Modification of routing by location
2.9	Provide the ability for the administrator/supervisor to amend the skills associated with a given call agent
2.10	Provide the ability for the administrator/supervisor to configure at least 10% of agent positions with the capability of having two headsets
2.11	Provide the ability to automatically disconnect after hours calls after the announcement
2.12	Provide the ability to automatically or manually route after hours calls to the Weekends, Holidays, Evenings, and Nights (WHEN) customer care or other numbers as required
2.13	Provide the ability to inform the Veteran when their afterhours call has been routed to the WHEN customer care or other agent
2.14	Provide the ability for the call agent and administrator/supervisor to log-into the system by using an ID number or specified log-on key on the instrument (agents shall also be able to log in via computer in lieu of instrument)
2.15	Provide the ability for the call agent and administrator/supervisor to log out of the system
2.16	Provide the ability for call agents to designate various work statuses on their phones (for example, ready, work, break, special project, supervision, training, etc.)
2.17	Provide the ability to notify the user of the status of calls on a real-time basis
2.18	Provide the ability to notify the user (audio and/or visual) that there is a call waiting in the queue
2.19	Provide the ability for the administrator/supervisor to notify (audio and/or visual) agents that there is a call(s) in the queue
2.20	Provide the ability for agents to refer callers to voice mail or other service options
3.0	Provide the ability for the caller to utilize the following IVR capabilities
3.1	Provide the ability for the caller to utilize self-service options through touch tone (the caller selects the number that corresponds to the option that they want), directed speech (recording of predetermined options and the caller speaks the option that they want), and text to speech (English and Spanish keywords shall be recognized)
3.2	Provide the ability to utilize native language spoken by the caller to route the call to the correct office/department or agent (English and Spanish keywords shall be recognized)
3.3	Provide the ability for the caller to hear IVR options presented using Directed

Identifier	EVS PoC ACD Feature
	Voice (computer generated voice) for selected Line of Business (LOB) segments
3.4	Provide the ability for up to nine (9) IVR calling trees per site
3.5	Provide the ability for the caller to replay the options multiple times
3.6	Provide the ability for callers who are waiting in the queue or on hold to hear announcements
3.7	Provide the ability to notify caller their call may be monitored or recorded
3.8	Provide the ability for the administrator/supervisor to configure the ACD and IVR and restrict specific features certain administrators/supervisors can configure (done by the lead administrator/supervisor)
3.9	Provide the ability for the administrator/supervisor to update general information and announcements to callers
3.10	Provide the ability for VA personnel to configure a message and routing point to be used in emergency situations
3.11	Provide the ability for the administrator/supervisor to add, delete, and change IVR options
3.12	Provide administrators/supervisors with Remote Audio Update (RAU) capabilities to add, delete, and change messages associated with IVR menus and toll free numbers
3.13	Provide the ability for the administrator/supervisor to add, delete, and change IVR routing exit points
3.14	Provide the ability for the administrator/supervisor to add and delete IVR tiers presented to the caller (each tier has multiple options for the caller to select)
3.15	Provide the ability for administrators/supervisors to input new information or broadcast messages that update the IVR in real time
3.16	Provide the ability for the administrator/supervisor to implement editorial changes in the IVR on a 24 hour/7 days a week basis
3.17	Provide the ability for the administrator/supervisor to use the IVR to play music to the callers waiting in the queue
3.18	Provide the ability to play the music immediately following the initial and delay announcements and whenever a call is on hold
3.19	Provide the ability for the administrator/supervisor to record announcements that will be played to the callers
3.20	Provide the ability for the administrator/supervisor to turn-off the speech self-service features
3.21	Provide the ability for the administrator/supervisor to turn-on the speech self-service features
3.22	Provide the ability for the caller to request a call back
3.23	Provide the ability for the administrator/supervisor to gather information about how the caller uses the IVR
3.24	Provide the ability for the administrator/supervisor to retrieve caller responses to IVR self-service
3.25	Provide the ability for the inbound caller (Veteran, family member or advocate) to

Identifier	EVS PoC ACD Feature
	identify themselves using a unique identifier provided by the caller
3.26	Provide the user the ability to view information about the identity of the inbound caller if relevant information about the caller is already available in the system
3.27	Provide CTI functionality to prepopulate caller information, scheduled appointments, etc. (desktop environment includes Windows XP, Windows 7, Apple Lion and Citrix)
3.28	Provide the ability to use the recorded caller's response to route the call to the appropriate agent/customer care/area
3.29	Provide the ability for the caller to access the knowledge management system from the IVR
4.0	Provide the ability for the administrator/supervisor to monitor agent calls on a real-time basis (ability to remotely monitor calls shall be provided)
4.1	Provide the ability for each administrator/supervisor to listen in on a telephone conversation between an agent and outside caller
4.2	Provide the ability for the service observation feature to operate silently and not give an indication of monitoring by audible clicks, changes in volume
4.3	Provide the ability to notify the agent that his/her call is being monitored
4.4	Provide the ability for the administrator/supervisor to turn-off the agent notification that his/her call is being monitored
4.5	Provide the ability for the administrator/supervisor to barge in and take over a call from a call agent
4.6	Provide the ability for the call agent to alert an administrator/supervisor that assistance is needed
4.7	Provide the ability for the administrator/supervisor to continuously monitor an agent's call, rather than monitoring a specific call
4.8	Provide the ability to alert the administrator/supervisor when a call agent is not available for longer than the specified period of time
4.9	Provide the ability for the call agent and administrator/supervisor to view the number of calls in the queue (wall mounted board and/or rolling electronic desktop view)
4.10	Provide the ability for the call agent and administrator/supervisor to view the length of time calls have been waiting in the queue (wall mounted board and/or rolling electronic desktop view)
4.11	Provide the ability for all call agents and administrator/supervisors to hear the number of calls in the queue
4.12	Provide the ability for all call agents and administrator/supervisors to hear the length of time calls have been waiting in the queue
5.0	Provide callers the ability to use automated call back features
5.1	Provide the ability for site to manage call back process, allowing agents to manually call back a number left in call back queue or have the system automatically call the first person in the call back queue when an agent becomes available

Identifier	EVS PoC ACD Feature
5.2	Provide the ability for the caller to hang-up the call, but remain in the queue (virtual queue) and receive a call back when he/she reaches the first position in the queue
5.3	Provide the ability to allow the caller to schedule the time of the call back at a specific telephone number
5.4	Provide the ability to configure the trigger point for the automated call back feature based upon time of day, maximum wait time, average wait time
5.5	Provide the ability for the automated call back feature to ask the caller to verify his/her identity
5.6	Provide the ability for the automated call back feature to allow sufficient time once the call has been answered for the caller to reach the handset
5.7	Provide the ability for the automated call back feature to provide the option to the individual who answers the call to be called back in 15 (configurable) minutes (up to 2 times-configurable)
5.8	Provide the ability for the automated call back feature to capture the incoming call number (Automatic Number Identification (ANI))
5.9	Provide the ability for the caller to enter a defined call back number for the automated call back feature to use
5.10	Provide the ability for the automated call back feature to capture current caller numbers for phones that are not Dual Tone Multi Frequency (DTMF) (not touch tone phones)
5.11	Provide the ability for the automated call back feature to capture current caller numbers of phones that use extensions
5.12	Provide the ability for VA personal to build a list of incoming phone numbers (ANI's) that can be blocked from call back in future by the automated call back feature. NOTE - This feature is to prevent prank calls, or abuse of the system
5.13	Provide the ability for the administrator/supervisor to prevent automated international call backs
5.14	Provide the ability for the administrator/supervisor to restrict automated call back feature to for certain area codes (900, 977, etc.)
5.15	Provide the ability for the systems administrator to configure the number of automated redial attempts that the call back feature will conduct in the event that a call back is unanswered or is routed to a fax machine
5.16	Provide the ability for the automated call back feature to leave a personalized recorded message if the call is not answered within a predefined number of attempts
5.17	Provide the ability for the administrator/supervisor to turn off the automated call back feature
5.18	Provide the ability for the administrator/supervisor to view/print a report of automated call back features including:
5.19	Total calls utilizing virtual hold
5.20	Estimated wait time vs. actual wait time for first attempted call back

Identifier	EVS PoC ACD Feature
5.21	Acceptance rate (caller acceptance of the offer of a call back) vs. stated queue depth (threshold of when the call back feature is offered as established by organization)
5.22	Provide the ability for the administrator/supervisor to prevent scheduled call backs under the following conditions:
5.23	Telephone Management Application (TMA) and date
5.24	Projected busy times
5.25	When offices are closed
5.26	Provide the ability for the automated call back feature to offer the caller a recommended time slot for a call back
5.27	Provide the ability for administrator/supervisor to view/print a report of failed automated call back attempts (document attempts to call back Veteran)
5.28	Provide the ability for the caller to specify the time zone that he/she wants the call returned
5.29	Provide the ability for the automated call back feature to accommodate callers in multiple time zones by estimating the time zone of the caller based on ANI (may be incorrect because of cell phones or other routing issues)
5.30	Provide the ability to create reports of individual call back attempts including date/time call was scheduled; reconnect attempts, successful connection date/time.
6.0	Provide the ability for the administrator/supervisor to record all calls within a specified work group for example a customer care group but exclude patient telephone calls, if required (all agents at all sites need ability to be recorded and kept for the life of the contract, including option years)
6.1	Provide the ability for the administrator/supervisor to listen to audio recordings 100% of the time
6.2	Provide the ability for the administrator/supervisor to view screen recordings of customer care agents 25% of the time (all agents at all sites need ability to have screens recorded, recordings shall be kept for the life of the contract, including option years)
6.3	Provide the Administrator/Supervisor with the ability to silently monitor a call without the party being aware
6.4	Provide the ability to record the calls of agents to a specific file format (wav/mp3, etc.) and sent to a VA.gov email address only through Microsoft Exchange. Exchange shall flag all emails as non- forwardable
6.5	Provide the ability to record a call based on a key sequence on the phone
6.6	Provide the ability to announce the call is being recorded and hear an audible beep when the key sequence is initiated on the phone
6.7	Provide the ability for the recording to be an undetermined amount of time
6.8	Provide the ability for the administrator/supervisor to delete Personally Identifiable Information (PII) from recordings to enable their use for training purposes

Identifier	EVS PoC ACD Feature
6.9	Provide the ability for the administrator/supervisor and other potential users to replay call recordings
6.10	Provide the ability for the administrator/supervisor to synchronize audio and screen recordings
6.11	Provide the ability for the administrator/supervisor to search for specific key words in a recording, for example the phrase "call back"
6.12	Provide the ability for the administrator/supervisor to have a live recording of a conversation sent to his/her mailbox
6.13	Provide the ability for the administrator/supervisor to search and monitor calls using the incoming call number, agent, or team designations
6.14	Provide the ability for the administrator/supervisor to create custom call quality evaluation forms
6.15	Provide the ability for the administrator/supervisor to forward agent call recording evaluations to agent for review
6.16	Provide the ability for the administrator/supervisor to flag recordings as best call example, complaint, threat, special issue, etc.
6.17	Provide ability for the administrator/supervisor to search, retrieve, and play recorded messages for defined historical period (the life of the contract, including option years)
6.18	Provide the ability to include caller detail information along with the recording - IVR exit point, time in queue, talk time, transfers, hold time, etc.
7.0	Provide the ability for the administrator/supervisor to generate management reports
7.1	Provide the ability for the administrator/supervisor to view on screen/print reports generated on a predetermined schedule, such as daily, weekly or monthly
7.2	Provide the ability for the administrator/supervisor to view on screen/print reports on demand
7.3	Provide the ability for the administrator/supervisor to view/print reports remotely
7.4	Provide the ability for the administrator/supervisor to view on screen/print reports by hours of operation determined by VA for site, week, or month
7.5	Provide the ability for the administrator/supervisor to view on screen/print report of call information for a minimum of 100 days and maximum of the life the contract with the option to export data outside of the system
7.6	Provide the ability for the administrator/supervisor to create a report of call information older than 100 days
7.7	Provide the ability for the administrator/supervisor to view/print agent and line reports containing the following information:
7.8	Number of calls received on each individual line
7.9	Number of calls received on each individual trunk group
7.10	Number of calls placed on each individual line
7.11	Number of calls placed on each individual trunk group
7.12	Time in-use of inbound circuits

Identifier	EVS PoC ACD Feature
7.13	Time in-use of outbound circuits
7.14	Number of calls abandoned from queue for the total number of inbound circuits
7.15	Number of incoming calls handled by each agent, identified by employee name and/or employee ID number
7.16	Number of outgoing calls handled by each agent, identified by employee name and/or employee ID number
7.17	Actual call handles time by agent identified by employee name and/or employee ID number
7.18	Actual call wrap-up time by agent identified by employee name and/or employee ID number
7.19	Average call handle time by agent identified by employee name and/or employee ID
7.20	Call Wait Time - The number of calls by queue that waited over a specified number of seconds to be answered
7.21	Percentage of calls that waited over a specified period of time
7.22	Average speed of answer for each queue
7.23	Average speed of answer for an individual call agent
7.24	Average speed of answer for the customer care agent
7.25	Number of calls placed on hold by agent identified by an employee name and/or ID number
7.26	Average number of calls placed on hold by agent identified by an employee name and/or ID number
7.27	Number of calls placed on hold by queue
7.28	Average number of calls placed on hold by queue
7.29	Number of calls placed on hold by a customer care group
7.30	Average number of calls placed on hold by customer care group
7.31	Which option(s) are selected from the main hospital greeting
7.32	Time when a call agent has indicated that they are not available to take calls (on a break, in training, etc.)
7.33	Number of incoming abandoned calls (Abandon Wait Time Buckets Summary) in seconds
7.34	Percentage of incoming abandoned calls
7.35	Cumulative percentage of incoming abandoned calls by day, month, year, and days of the week
7.36	Number of transferred calls by the individual call agent and/or for customer care group
7.37	Average amount of time when a caller leaves a message for a call back and when the call is actually made back to the caller and the caller is reached/connected
7.38	Average amount of time when a caller leaves a message for a call back and when the call is actually made back to the caller and the caller is not reached
7.39	Average amount of time when a caller leaves a message for a call back and when the call is actually made back to the caller and the caller is either reached or not reached

Identifier	EVS PoC ACD Feature
7.40	Provide the ability for the administrator/supervisor to generate agent activity reports to include:
7.41	Number of internal calls answered
7.42	Average talk time duration for internal calls
7.43	Total talk duration
7.44	Number of times agent entered into work mode
7.45	Average duration of break mode by agent
7.46	Length of time a message was left in a queue requesting a call back and when the call was actually returned
7.47	Length of time a call in a queue was actually returned
7.48	Reports to be generated on a daily, weekly, monthly, yearly, and days of the week
7.49	Reports can be generated by the following intervals: 15 minutes, 30 minutes, 1 hour
7.50	Provide the ability for call agent to identify type of call routed at end of call
7.51	Provide the ability for the administrator/supervisor to create reports on type of call routed
7.52	Provide the ability for the administrator/supervisor to change the specified period of time period to suit individual requirements
7.53	Provide the ability for the administrator/supervisor to adjust the parameters of all reports
7.54	Provide the ability for the administrator/supervisor to generate system summary reports by queue
7.55	Provide the ability for the administrator/supervisor to specify/configure the interval at which a system summary report by queue is generated
7.56	Provide the ability for the system to generate the following system summary reports for the administrator/ supervisor to access:
7.57	Total number of incoming calls
7.58	Number of calls answered
7.59	Number of calls in queue
7.60	Number of abandoned calls
7.61	Number of calls offered to the system
7.62	Number of outbound calls
7.63	Average talk time
7.64	Average time in queue
7.65	Average waiting time until abandoned
7.66	Average waiting time until answered
7.67	Average outgoing call conversation time
7.68	Blockage Rate for incoming calls to center/facility and per individual queue
7.69	Blockage Rate for incoming calls per individual queue
7.70	Provide the ability for the administrator/supervisor to generate reports by customer care location, region, or queue
7.71	Provide the ability for the administrator/supervisor to simultaneously receive

Identifier	EVS PoC ACD Feature
	information about groups of agents and the groups within the queue
7.72	Provide the ability for the administrator/supervisor to print reports from the Management Information Systems (MIS) Graphical User Interface (GUI) access console or Personal Computer (PC)
8.0	Provide the ability for the administrator/supervisor to generate infrastructure monitoring and reporting
8.1	Provide the ability for the administrator/supervisor to print on demand line reports or view to include a list of all equipment alarms, error tables, trouble logs, and history file
8.2	Provide the ability for the administrator/supervisor to automatically receive printed line reports on a predetermined schedule to include a list of all equipment alarms, error tables, trouble logs, and history file
8.3	Provide the ability for the administrator/supervisor to remotely generate an electronic work order for trouble reports, moves, additions and changes
8.4	Provide the ability for the administrator/supervisor to direct work orders to internal and external recipients, depending upon the nature of the problem and whether or not it will be addressed by VA staff or contractors
8.5	Provide the ability for work order report to include:
8.6	Location of the issue
8.7	Type of equipment associated with the issue
8.8	Provide the ability for the administrator/supervisor to create a phone bill report
9.0	Provide the ability for the systems administrator to generate reports
9.1	Provide the ability for the systems administrator to generate phone line capacity reports
9.2	Provide the ability for the systems administrator to generate quality of service reports (static on line, bad connections, etc.)
10	Provide the ability to collect internal (VA employees) and external (The Veteran) caller customer satisfaction information.
10.1	Caller Interaction with Customer Satisfaction Survey
10.2	Provide the ability to offer the customer satisfaction survey to callers just prior to connection to the agent, not before queuing, to reduce the chance of abandonment.
10.3	Provide the ability to offer the customer satisfaction survey to callers to be completed at the following times.
10.4	Immediately after callers have finished inaction with the call agent or VA representative.
10.5	At a later date specified by callers resulting in a scheduled call back.
10.6	Provide the ability for the caller to request a scheduled call back up to five days after the initial call was received.
10.7	Provide the ability for the caller to be informed of what area is being assessed in the customer satisfaction survey when a call back is used to deliver the survey.
10.8	Provide the ability for the caller to opt out of the customer satisfaction survey

Identifier	EVS PoC ACD Feature
	at the following times:
10.9	The offer is initiated.
10.10	Prior to commencement of the survey.
10.11	Provide the ability for the caller to respond to the customer satisfaction survey questions using touch tone, voice inputs and technologies to ensure 508 Compliance.
10.12	Provide the ability for the caller to provide comments (recordings) after each question and overall if desired.
10.13	Provide the ability for the caller to leave an audio recorded message up to 3 minutes in duration at the end of the customer satisfaction survey for general comments.
10.14	System Administration Configuration Capabilities for Call Survey
10.15	Provide the administrator/supervisor the ability to configure the customer satisfaction survey offer rate.
10.16	Provide the administrator/supervisor the ability to configure the customer satisfaction survey based on call type determined by skill set for call.
10.17	Provide the administrator/supervisor the ability to configure the customer satisfaction survey based on call type determined by business lines.
10.18	Provide the administrator/supervisor the ability to configure the offer rate of the customer satisfaction survey in % increments to up to 100% of callers if desired.
10.19	Provide the administrator/supervisor the ability to draft up to 15 questions per customer satisfaction survey
10.20	Provide the administrator/supervisor the ability to specify the number of questions up to 15 that the caller is asked as part of customer satisfaction survey.
10.21	Provide the administrator/supervisor the ability to create up to 25 concurrent customer satisfaction surveys to be stored for active use in the system (25 per site).
10.22	Provide the administrator/supervisor the ability to archive customer satisfaction surveys and associated call data for future analysis.
10.23	Provide the administrator/supervisor the ability to associate surveys to call types.
10.24	Provide the administrator/supervisor the ability to carry out audio updates remotely using both natural speech and text to speech systems. (English and Spanish shall be recognized)
10.25	Provide the administrator/supervisor the ability configure user access permissions for the systems associated with the customer satisfaction survey.
10.26	Provide the administrator/supervisor the ability to preview the customer satisfaction surveys.
10.27	Provide the administrator/supervisor the ability to remotely access the customer satisfaction survey management system.
10.28	Provide the ability for administrators and managers/supervisors to generate real-time reports at the enterprise, queue, hunt group, and supervisor group levels
10.29	Provide the ability for administrators and managers/supervisors to manually and automatically generate historical ACD reporting at the interval, daily, weekly, and

Identifier	EVS PoC ACD Feature
	monthly level and real-time reporting at the interval and daily level
10.30	Provide the administrator/supervisor the ability to configure customer satisfaction survey reporting results, down to a minimum of 30 minute segments, and up to a minimum of one year of results.
10.31	Provide the administrator/supervisor the ability to generate a customer satisfaction survey report with the following data:
10.32	Record associated caller data (ANI).
10.33	Original call data (date, time, agent, IVR exit point).
10.34	Survey results of the caller.
10.35	Based on agent and call level
10.36	Caller general comment categories
10.37	Provide the administrator/supervisor the ability to define groups of users/agencies or questions to apply to customer satisfaction survey results for reporting purposes.
10.38	Provide the administrator/supervisor the ability to sort, sum, and average customer satisfaction survey responses over a custom time range
10.39	Provide the administrator/supervisor the ability to sort, sum, and average responses by organizational hierarchies from agent level to Agency level
10.40	Provide the administrator/supervisor the ability to allocate categories such as, compliment, general or complaint to Veteran General comments that were made during the customer satisfaction survey.
10.41	Provide the administrator/supervisor the ability for exporting of customer satisfaction survey responses into Comma Separated Values (CSV) or similar format for use with Microsoft Suite products.
10.42	Provide the administrator/supervisor the ability to create graphical displays for each customer satisfaction survey question using custom time ranges.
10.43	Provide the administrator/supervisor with the ability to analyze customer satisfaction survey data using statistical functions such as average, mean, median, and standard deviation.
10.44	Provide the administrator/supervisor the ability to generate reports on the interaction of the Veteran with the customer satisfaction survey to include:
10.45	Survey acceptance.
10.46	Survey connection rate.
10.47	Survey completion rates.
10.48	System shall provide access to respondent comments.
10.49	Percent Sessions Answered (PSA).
10.50	Average Handle Time (AHT) in Hour Hour: Minute Minute: Second Second (HH:MM:SS).
10.51	The percent of time the targeted service objective was met.
10.52	Busies/failed contact.
10.53	Average Speed of Answer (ASA).
10.54	Provide the administrator/supervisor the ability to configure the sampling interval at which data for the interaction of the caller with the customer satisfaction survey

Identifier	EVS PoC ACD Feature
	report is collected by the system.
10.55	Provide the administrator/supervisor the ability to configure the reporting period for the reports concerning the interaction of the caller with the customer satisfaction survey.
10.56	Provide the ability for the administrator/supervisor to view/print the following caller details along with the survey results: incoming call number (ANI), amount of time in queue, agent ID, customer care, IVR exit point, talk time, transfers, etc.

D.9.0 ANALOG SERVICES

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide the necessary licenses, analog line cards and sufficient hardware to support analog services for patient phones, fax machines, elevator lines, credit card authorization lines and any other analog service requirements. The analog phones shall allow patients to receive calls and make local calls only. Long distance calls shall be restricted and, if required, shall be connected through the operator.

D.10.0 SOFT PHONES

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide soft phone capability as part of EVS PoC. Soft phones shall enable VA users to perform telephony functions from a remote desktop or laptop computer in the event a user has the need to Telework in addition to their regular desk phone. The softphone application shall allow the user to have identical services, functionality, and button layout to their desktop telephone, with the exception of E911 capabilities. The Contractor shall disable E911 capability from the softphones when the user is working at a location other than their regular VA office. The Contractor shall provide labels to be attached to desktops or laptops on which the softphone application is installed. The label shall explicitly instruct the user to not call 911 from the softphone when working remotely. Softphone onsite availability shall meet the same requirements as a desk phone; softphone via remote VPN access will not be held to the same availability standard.

D.11.0 DIAL PLAN

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall retain the existing telephone numbers and current internal dial plans. This shall include toll free, main and local directory numbers, customer care direct numbers, Direct Inward Dials (DID's) and any other site specific advertised direct access numbers, as well as additional items identified in the addendums and site survey.

The EVS PoC solution shall incorporate the standard dial plan that is currently in use by each site to prevent future difficulties in the development of the Enterprise Dial Plan. The current dialing structure shall be as follows:

a. Provide centralized toll free access through switchboard to all CBOCs and Vet Centers b. Dial outside to PSTN – Dial "9" and the 10 digit number

b. Dial within the VISN – Dial “8” and then the seven (7) digit number

c. nternal On Net dialing – Dial four (4) digit extension

d. Dial "0" to reach operator services at facilities

D.12.0 LONG DISTANCE AUTHORIZATION

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide the capability for authorization codes to allow for long distance and international dialing. Long distance dialing shall be managed by providing each user with a dialing code. The Contractor shall support existing VISN PIN codes and support user mobility between locations within the VISN. The Contractor shall provide the ability to authorize temporary PIN codes (for a specific length of time set by VA) for visitors or accommodate visitor PIN codes from other VISN sites.

D.13.0 CALL DETAIL RECORDS (CDR)

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide Call Detail Records (CDR) which captures a record of each call made or received. Traffic Accounting and Management of CDRs shall be provided for each call. This shall include complete records of all calls completed with an associated Personal Identification Number (PIN) dialing control. EVS PoC shall be capable of gathering call detail report data for VoIP trunks and stations. CDR records may be destroyed when 3 years old. CDRs may be destroyed earlier if the information needed to identify abuse has been captured in other records.

The call detail record shall be composed of data fields that describe the telecommunication transaction, such as:

a. Phone number of the subscriber originating the call (calling party)

b. Phone number receiving the call (called party)

c. Starting time of the call (date and time)

d. Call duration

e. Billing phone number that is charged for the call

f. Identification of the telephone exchange or equipment writing the record

g. Sequence number identifying the record

h. Additional digits on the called number used to route or charge the call

i. Disposition or the results of the call, indicating for example whether the called party was busy, or the call failed the route by which the call entered the exchange

j. Route by which the call left the exchange

k. Call type (voice, SMS, etc.)

l. Fault condition encountered

m. 24-hour web enabled access capability to retrieve and capture call detail records.

n. Ad hoc reports

D.14.0 ADDITIONAL GENERAL VOICE FEATURES

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide the capability to support emerging/converged technologies, such as UC and related applications and be scalable. The EVS PoC solution shall integrate with applications such as IVR, call recording, and other capabilities (as captured during a site survey), e.g., call message detail, music on hold, virtual hold, overhead, long and short range paging equipment, Nurse Call, dial dictation, and E911.

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide a solution that interfaces with a centralized dial dictation system and shall provide the same features, functions, and services as presently provided. Selected station users shall have access to the centralized dictation system by dialing the proper access code. Any optional CLIN performed by the Contractor shall have the capability of transmitting DTMF signals for control, such as, review, fast forward, playback. The Contractor shall identify the dial dictation equipment/service, if any, used at each location. The Contractor shall coordinate with the company currently providing the dial dictation equipment/service and VA to identify interface requirements (type device, tone or pulse, for example) with EVS PoC. As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide and install any required interface device. VA will be responsible for providing the interface device, if it is a card or option in the dictating equipment. The telephone system shall provide a feature to prevent the dictation system from being "locked up" by a user putting the system on hold or leaving the receiver "off-hook". The Contractor shall provide the cable and terminals between the telephone equipment room and the dial dictation equipment room.

As part of any optional CLINs the Contractor is tasked to perform, the Contractor shall provide the EVS PoC capabilities in the table below.

Identifier	EVS PoC Feature
1.0	Provide common user/agent desktop features via EVS PoC telephony
1.1	Provide the ability for the end user to take the following actions to process incoming and outgoing calls:
1.2	Forward a call
1.3	Place a call on hold
1.4	Resume a call that has been placed on hold
1.5	Request an audible alert when call has been on-hold for a specified period of time
1.6	Configure the length of on-hold time
1.7	Call Park (place call on hold on one phone and pick-up call on another phone)
1.8	Answer a call (Call Pickup)
1.9	Answer a group call
1.10	Transfer calls outside of the facility (example hospital to Community-Based

Identifier	EVS PoC Feature
	Outpatient Clinic (CBOC)) and within the facility (another extension within facility)
1.11	Have an option as a class of service to perform "warm" transfer (verbally handing off caller details to the next agent)
1.12	Have an option as a class of service to transfer and/or forward assigned extension to another device (i.e., BlackBerry, cell phone, etc.)
1.13	Allow authorized users to make long distance calls without having to enter a code
1.14	Block or restrict long distance calls
1.15	Make international calls
1.16	Block/restrict international calls
1.17	Ability to call on-network between all VA – Individual Site locations – X-digit dialing
1.18	Provide the ability for VA staff to use the following interface features:
1.19	Hands-free speakerphone
1.20	Voice dialing
1.21	Audible and visual indication of ringing line
1.22	Call Status per line
1.23	Map-able Soft Keys
1.24	Answer/Release
1.25	Mute a call
1.26	Have the ability for a supervisor/manager to barge in or completely intercept a call if necessary
1.27	Have the ability for a supervisor/manager to record the calls / media streams for a specific number or range of numbers. Calls can also be recorded at the trunk or station level.
1.28	Hear/view audible and visual alert when call is muted
1.29	Identification of inbound caller with display (Caller ID)
1.30	Caller/contact information displayed on desktop for incoming call
1.31	Designate which caller identification number will display (specific clinic or main clinic number main facility by default, allow for per line as required)
1.32	Block display of a phone number (for example a call made from investigative services)
1.33	View the telephone numbers of the last 10 calls received by a specific phone
1.34	Provide the following standard handset functionality: minimum of 3 call appearances
1.35	Provide the ability for the VA staff to utilize the following conferencing features
1.36	Internal/external local site ad hoc conferencing
1.37	Local site multi-party meet me/ad hoc conferencing to accommodate up to eight (8) participants (eight concurrent conferences per site)
1.38	No hold transfer or no hold conference (no audible beep heard when entering active line)
1.39	Local site secure conferencing through the use of a PIN
1.40	Local site conference chaining (the ability to another conference into a conference call)

Identifier	EVS PoC Feature
1.41	Provide the ability for VA staff to use the following directories:
1.42	Personal address book
1.43	VA directories (Global Address List integration)
1.44	Provide the agent or person making or receiving the call with the ability to receive the call through an interface with a desk or wall mounted push button telephone hand set
1.45	Provide the agent or person making or receiving a call with the ability to use software based phone client running on an appropriately configured computer by plugging in a headset into an appropriate computer port (Universal Serial Bus (USB) port or audio port)
1.46	Provide the ability to use either a handset receiver and/or headset to communicate (two jacks on device)
2.0	Voicemail Features
2.1	Provide the ability for VA staff to take the following voice mail actions
2.2	Record at least 5 personal greetings
2.3	Select a specific greeting for playback
2.4	Create internal and external greetings
2.5	Specify after-greeting action(s)
2.6	Send a message to a specific user or phone number that caller is requesting a response
2.7	Create private distribution list and send messages to this list
2.8	Mark messages as regular, urgent, or private
2.9	Play messages
2.10	Process/disposition messages
2.11	Address message to multiple recipients
2.12	Search for messages by name of caller, caller identification (ID), phone number, and extension
2.13	Create secure messages (no playback when sent outside of organization)
2.14	Request return receipts for recorded messages
2.15	Live reply (Internal and external callers) - immediately reply to messages
2.16	Forward message to specified individual or agent
2.17	Save voice mail to e-mail/ integrate voice mail with email. All e-mails shall be FIPS 140-2 encrypted as there is a possibility of PII or PHI information being left in the voicemails. All e-mails are to be sent to VA.GOV e-mail addresses only; no external VA e-mail addresses can be utilized. Any email messages received from the voicemail system shall be flagged as non-forwardable by the Microsoft Exchange server
2.18	Allow the caller to skip the greeting and record a message
2.19	After recording a message, get out of voice mail and back into queue or back to an operator
2.20	Use certain codes/numbers to fast forward, skip messages, replay a message, etc.
2.21	Turn-off or not assign a voice mail to a specific extension (caller will not be able to

Identifier	EVS PoC Feature
	leave voice mail)
2.22	Password protect user voice mail
2.23	Display visual and provide audible indication that a message is waiting
2.24	Provide the ability for VA staff/provider to leave a secure message for a caller
2.25	Provide the ability for the caller to retrieve the secure message left by the VA staff/provider
2.26	Provide the ability for the administrator/supervisor to take the following voice mail actions
2.27	Provide the ability for the administrator/supervisor to set size of mail box for an individual user (at a minimum of thirty (30) messages or 260 seconds total)
2.28	Provide the ability for the administrator/supervisor to increase the size of a mail box for a clinic (voice messages for all sites shall be restricted to a maximum of 3 minutes in length, with the option to change message length by administrator)
2.29	Provide the ability for the administrator to delete a user's mail box
2.30	Provide the ability for the administrator to set/reset a user's password
2.31	Provide the ability for the administrator to establish team voice mail mailboxes
2.32	Provide the ability for the administrator/supervisor to view status of played and unplayed messages, pull reports on weekly, monthly, or ad hoc basis
3.0	Provide the ability to integrate use of the EVS PoC system with use of local applications. (desktop environment includes Windows XP, Windows 7, Apple Lion and Citrix)
3.1	Provide the ability to integrate use of EVS PoC telephony with use of the Nurse call systems
3.2	Provide the ability to integrate use of EVS PoC telephony with use of the paging systems (overhead) including dial to page feature for intercom system and a direct dial to intercom to phone sets
3.3	Provide the ability to integrate telemetry systems into EVS PoC
3.4	Provide the ability to integrate televideo/telepresence systems into the EVS PoC solution (Optional CLIN, see Section 5.10)
3.5	Provide the ability to integrate use of EVS PoC telephony with audio care systems.
3.6	Provide the ability to "blast" a message to all registered users in the event of an emergency
3.7	Provide the ability to integrate use of EVS PoC telephony with use of fax systems (analog fax machines and fax servers)
3.8	Provide the ability to integrate use of EVS PoC telephony with use of wireless extended handsets (handsets shall be FIPS 140-2 compliant) (Optional CLIN, see Section 5.11)
3.9	Provide ability for wireless capable handsets (FIPS 140-2 compliant) to roam to another facility and obtain local dial tone and update location based services (including E911 information)
3.10	Provide the ability to integrate use of EVS PoC telephony with instant messaging, text, and chat.

Identifier	EVS PoC Feature
3.11	Provide the ability to integrate use of EVS PoC telephony with use of Microsoft Communicator (now Microsoft Lync) to deliver voice presence
3.12	Provide the ability to integrate presence sensing tools (Global Positioning System (GPS) into the EVS PoC solution
3.13	Provide the ability to integrate use of EVS PoC with use of facility security systems such as fire and security alarm services
3.14	Provide the ability to integrate facility management systems into the EVS PoC solution
3.15	Provide the ability to integrate use of EVS PoC telephony with use of the exchange mail system.
3.16	Provide the ability to integrate use of EVS PoC telephony with use of emergency elevator phones.
3.17	Provide the ability to dial using E.164 as well as alphanumeric SIP Uniform Resource Identifiers (URIs) dialing.

ADDENDUM E – SUPPLEMENTARY INFORMATION

E.1.0 LIST OF VA TOOLS AVAILABLE FOR MANAGEMENT, MONTIORING, AND REPORTING

The Contractor shall make use of VA tools as specified in this PWS. These applications are listed below. This list is not exhaustive; VA may make other tools available during the period of performance.

- SolarWinds
- ScienceLogic
- Splunk
- SFTP
- CA Service Desk Manager
- syslog

E.2.0 ACRONYMS

Acronyms used throughout this document can be found below, or at VA Acronym Lookup.

Abbreviation	Meaning
A&A	Assessment and Authorization
ACD	Automatic Call Distributor
ANI	Automatic Number Identification
ATO	Authority to Operate
ATP	Acceptance Test Plan
BCM	Business Capacity Management
BCP	Business Continuity Plan
BP	Build Package
BRI	Basic Rate Interface
CA	Computer Associates
CBOC	Community Based Outpatient Clinic
CDB	Continuity Database
CDCO	Corporate Data Center Office
CDP	Cisco Discovery Protocol
CDR	Call Detail Record

Abbreviation	Meaning
CERT	Computer Emergency Response Team
CI	Configuration Item
CLIN	Contract Line Item Number
CMS	Change Management System or Configuration Management System
CMDB	Configuration Management Database
CO	Contracting Officer
ConOps	Concept of Operations
COOP	Continuity of Operations Plan
COR	Contracting Officer Representative
COS	Class of Service
COTS	Commercial Off-the-Shelf
CPMP	Contractor Project Management Plan
CPU	Central Processing Unit
CPX	Command Post Exercise
CRISP	Continuous Readiness in Information Security Program
DB	Database
DC	Direct Current
DDD	Direct Distance Dialing
DID	Direct Inward Dial
DNIS	Dialed Number Identification Service
DoW	Day of Week
DoY	Day of Year
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DTMF	Dual-Tone Multifrequency
E911	Enhanced 911 Emergency Services Number
EA	Enterprise Architecture
ECCB	Executive Change Control Board

Abbreviation	Meaning
ECMS	Enterprise Content Management System
ESE	Enterprise Systems Engineering
EVS PoC	Enterprise Voice System
EVTN	Enterprise Video Teleconferencing Network
FCD	Federal Continuity Directive
FCR	First Contact Resolution
FIFO	First In First Out
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FTX	Field Training Exercise or Full Function Exercise
GAL	Global Address List
GFE	Government Furnished Equipment
GRC	Governance, Risk, and Compliance
HF	High Frequency
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air Conditioning
IA	Information Assurance
ICF	Integrated Clinical Facility
IDDD	International Direct Distance Dialing
IMS	Integrated Master Schedule
IPv6	Internet Protocol Version 6
IS	Information System
ISO	Information Security Officer
ISCP	Information System Contingency Plan
ISCPA	Information System Contingency Planning Assessment
ISDN	Integrated Services Digital Network
IT	Information Technology

Abbreviation	Meaning
ITIL	Information Technology Information Library
ITSCM	Information Technology Service Continuity Management
ITSM	Information Technology Service Management
ITU	International Telecommunications Union
IVR	Interactive Voice Response
IXC	Interexchange Carrier
Kbps	Kilobits per second
KEDB	Known-Error Database
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LATA	Local Access and Transport Area.
LCD	Liquid Crystal Display
LEC	Local Exchange Carrier
LMR	Land Mobile Radio
LNP	Local Number Portability
MACD	Move, Add, Change, and Disconnect
MAN	Metropolitan Area Network
MGCP	Media Gateway Control Protocol
MHz	Megahertz
MMS	Multimedia Messaging Service
MOS	Mean Opinion Score
MOU	Memorandum of Understanding
MS	Microsoft
MSN	Memorial Service Network
MTBF	Mean Time Between Failures
MTD	Maximum Tolerable Downtime
MTRS	Mean Time to Restore Service
MTTR	Mean Time To Repair

Abbreviation	Meaning
NBD	Next Business Day
NCA	National Cemetery Administration
NCCB	National Change Control Board
NEC	National Electrical Code
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operations Center
NSD	National Service Desk
NSOC	Network and Security Operations Center
NSPD	National Security Presidential Directive
OCS	Office of Cyber Security
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMAPR	Operations, Maintenance, Administration, Provisioning, and Repair
OPC	Outpatient Clinic
PACT	Patient Aligned Care Team
PCT	Post Cutover Test
PHI	Protected Health Information
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PM	Program Manager or Project Manager
PMAS	Project Management Accountability System
PMO	Program Management Office

Abbreviation	Meaning
PO	Privacy Officer
POA&M	Plan of Action and Milestones
PoC	Proof of Concept or Point of Contact
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
PRI	Primary Rate Interface
PS/ALI	Private Switch / Automatic Location Identification
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PWS	Performance Work Statement
QoS	Quality of Service
RAU	Remote Audio Update
RBO	Regional Benefit Office
RCM	Resource Capacity Management
RDP	Regional Data Processing
RDPC	Regional Data Processing Center
RMP	Risk Management Plan
RP	Release Package
RPO	Recovery Point Objective
RSD	Requirements Specifications Document
RTO	Recovery Time Objective
SACM	Service Asset Configuration Management
SAT	System Availability Test
SCM	Service Capacity Management
SDD	System Design Document
SDM	Service Desk Manager
SEDR	System Engineering Design Review
SIP	Session Initiation Protocol

Abbreviation	Meaning
SLA	Service Level Agreement
SME	Subject Matter Expert
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSP	System Security Plan
TAA	Trade Agreements Act
TDD	Telecommunications Device for the Deaf
TDM	Time Division Multiplexing
TIA	Telecommunications Industry Association
TIC	Trusted Internet Connection
TMM	Total Minutes In The Month
TMS	Talent Management System
TMU	Total Minutes In Month Unavailable
TOD	Time of Day
TRM	Technical Reference Model
TTX	Tabletop Exercise
TTY	Teletype
UC	Unified Communications
UPS	Uninterruptable Power Supply
UT	Unit Testing
VA	Department of Veterans Affairs
VaaS	Voice as a Service
VAMC	VA Medical Center
VANTS	VA Nationwide Teleconferencing System
VBA	Veterans Benefits Administration
VCS	Version Control System or Video Communications Server
VHA	Veterans Health Administration
VHF	Very High Frequency

Abbreviation	Meaning
VISN	Veterans Integrated Service Network
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VRM	Veterans Relationship Management
WAN	Wide Area Network
WBS	Work Breakdown Structure
WFM	Workforce Management
WHEN	Weekend, Holiday, Evening, Night

E.3.0 DEFINITIONS

Terms used within this document are described below, or at OI&T Master Glossary.

Term	Definition
24x7	Twenty-Four Hours a Day, Seven Days a Week
Assessment and Authorization	The process by which an information system's risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, is assessed based on the implementation of an agreed-upon set of security controls; and a determination is made on whether or not an information system should be allowed to operate.
Authority to Operate	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Automatic Call Distributor	A system that distributes incoming calls to a specific group of telephones or agents based on customer need, type, and agent skill set.

Term	Definition
Automatic Number Identification	A method used by telephone companies to automatically identify and capture the telephone number of a call originator.
Basic Rate Interface	A 144 Kbps digital telecommunications access line, intended for home or small business use, that provides two 64 Kbps bearer channels and one 16 Kbps data channel. The bearer channels can be used for voice or data. The bearer channels can be combined to form a single 128 Kbps data connection.
Bit	A word blend of binary digit. The basic unit of information in computing and digital communications. A bit can have only one of two values commonly represented as 0 or 1.
Build Package	A package of changes that comprise a release; e.g., configuration items, delivery mechanisms, test plans, documentation, and training.
Business Capacity Management	The process by which both current and future, and strategic and tactical business requirements for IT service capacity are considered, planned, and implemented.
Business Continuity Plan	The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.
Call Detail Record	A data record produced by a telephone exchange or other telecommunications equipment that contains attributes that are specific to a single instance of a telephone call or other communication transaction that was handled by that facility or device
Central Processing Unit	The electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output operations specified by the instructions.
Change Management System	A set of tools, data and information that is used to support change management.
Class of Service	A method used to prioritize different types LAN traffic.
Command Post Exercise	A field exercise participated in by command, staff, and communication personnel only.
Commercial Off-the-Shelf	Pre-existing systems or applications available to the general public for purchase.
Computer Emergency Response Team	A computer security incident response team responsible for the prevention, detection, and remediation of cyber threats.

Term	Definition
Concept of Operations	A document that describes how an asset, system, or capability will be employed and supported. The concept of operations uses real-world business mission and operational scenarios to describe, in non-technical terms, a “Day in the Life” of the asset, system or capability. The scenarios are written or validated by the hands-on users who must perform operational tasks and functions. From these scenarios, needed capabilities can be derived and validated.
Configuration Item	Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements.
Configuration Management Database	A database used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items, and relationships with other configuration items.
Configuration Management System	A set of tools, data and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analyzing and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes and releases.
Continuity Database	A set of OI&T databases and toolkits that assist planners in complying with VA continuity requirements.
Continuity of Operations Plan	A predetermined set of instructions or procedures that describe how an organization’s mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
Continuous Readiness in Information Security Program	OI&T’s integrated approach to protect sensitive information from inappropriate exposure or loss.
Day	Unless otherwise specified, day means calendar day.

Term	Definition
Dialed Number Identification Service	A service provided by telecommunications companies that lets corporate clients determine which telephone number was dialed by a customer.
Direct Current	The unidirectional flow of electric charge. Direct current is produced by sources such as batteries, thermocouples, solar cells, and commutator-type electric machines of the dynamo type.
Direct Distance Dialing	A telephone network feature that allows a call originator, without operator assistance, to call any other telephone number outside the local calling area.
Direct Inward Dial	A feature offered by telephone companies which allows an individual extension on a private automated branch exchange to be reached directly via its own standard outside number.
Disaster Recovery	The processes and activities executed to restore an organization's critical business functions in the event of an interruption in service.
Disaster Recovery Plan	A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Dual-Tone Multifrequency	Used by push-button telephones for dialing, aka Touch-Tone.
Enterprise Architecture	An integrated framework that enables the evolution and maintenance of existing information technology systems and guides future technology acquisitions.
Enterprise Content Management System	VA's enterprise-wide content management system used to manage; e.g., coordinate, assemble, publish, and retire content; for VA's Internet and Intranet websites.
Executive Change Control Board	The ECCB operates at the IT Enterprise level of the Office of Information and Technology (OI&T). The purpose of the ECCB is to provide executive and technical leadership for enterprise change management and to support lower level change control boards (CCBs) in managing change requests that are escalated for ECCB review.
Field Training Exercise or Full Function Exercise	Field training exercises (FTXs) are used to practice continuity, contingency, and disaster recovery plans. FTXs provide fairly realistic scenarios and situations based on actual situations that may occur. The exercise is usually carefully planned out, and usually without disclosing plans or other information to exercise participants.

Term	Definition
First Contact Resolution	An industry recognized metric for measuring a Service Desk's ability to restore service to a user and close an incident during the first call or contact from the user.
First In First Out	A method for organizing and manipulating a data buffer, where the oldest (first) entry, or 'head' of the queue, is processed first.
Global Address List	Provides contact information for VA employees and contractors within Microsoft Outlook.
Hertz	The unit of frequency in the International System of Units (SI). It is defined as one cycle per second. One of its most common uses is the description of the sine wave, particularly those used in radio and audio applications, such as the frequency of musical tones.
High Frequency	A range of radio frequency electromagnetic waves (radio waves) between 3 and 30 MHz. Also known as the decameter band or decameter wave, because the wavelengths range from one to ten decameters (ten to one hundred meters).
Information Assurance	The practice of assuring the confidentiality, integrity, and availability of information; by managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.
Information Security Officer	The person responsible for information security at each VA Medical Center, and works in conjunction with Regional Information Security Officers (RISOs).
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Contingency Planning Assessment	A document which consolidates the results of a business impact assessment and threat and vulnerabilities assessments to facilitate the preparation of information technology contingency plans and the related training, testing, and exercises.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; e.g., computers, software, firmware, and similar related resources.

Term	Definition
Information Technology Information Library	A widely accepted approach to IT service management
Information Technology Service Continuity Management	A process responsible for managing risks that could seriously affect IT services. IT service continuity management ensures that the IT service provider can always provide minimum agreed service levels, by reducing the risk to an acceptable level and planning for the recovery of IT services. IT service continuity management supports business continuity management.
Information Technology Service Management	The implementation and management of quality IT services that meet the needs of the business. IT service management is performed by IT service providers through an appropriate mix of people, process and information technology.
Integrated Services Digital Network	A digital network standard for integrated voice and data network access, services, and user network messages.
Interactive Voice Response	A form of automatic call distribution that accepts user input, such as key presses and spoken commands, to identify the correct destination for incoming calls.
Interexchange Carrier	A U.S. legal and regulatory term for a telecommunications company, commonly called a long-distance telephone company, defined as any carrier that provides inter-LATA communication.
International Direct Distance Dialing	A feature of the public switched telephone network (PSTN) that enables a subscriber to dial an international telephone number directly, without the assistance of an operator.
International Telecommunications Union	An international committee that promotes international telecommunication standards.
Internet Protocol Version 6	The latest version of the Internet Protocol (IP); which provides a method to identify and locate computers on networks and routes traffic across the Internet.
Kilobits per second	A rate of data transmission where 1000 bits of information are sent each second.
Known Error	A problem that has a documented root cause and a workaround.
Known-Error Database	A database containing all known-error records.

Term	Definition
Land Mobile Radio	A land mobile radio system (LMRS) is a wireless communications system intended for use by terrestrial users in vehicles (mobiles) or on foot (portables); e.g., walkie-talkies and two way radios in vehicles.
Local Access and Transport Area	A contiguous geographic area within which a local telephone company (carrier) is permitted to offer telecommunications and telecommunications access services.
Local Area Network	A computer network that interconnects computers within a limited area such as a home, school, computer laboratory, or office building.
Local Exchange Carrier	A U.S. legal and regulatory term for a telecommunications company, commonly called a local telephone company, defined as any carrier that provides intra-LATA communication.
Local Number Portability	Also known as number portability and number porting, enables end users to keep their telephone number when switching from one telecommunications service provider to another.
Maximum Tolerable Downtime	The amount of time a mission/business process can be disrupted without causing significant harm to the organization's mission.
Mean Opinion Score	A test that has been used for decades in telephony networks to obtain the human user's view of the quality of the network.
Mean Time Between Failures	A metric for measuring and reporting reliability. MTBF is the average time that an IT service or other configuration item can perform its agreed function without interruption. This is measured from when the configuration item starts working, until it next fails.
Mean Time To Repair	The average time taken to repair an IT service or other configuration item after a failure. MTTR is measured from when the configuration item fails until it is repaired. MTTR does not include the time required to recover or restore. It is sometimes incorrectly used instead of mean time to restore service.
Mean Time to Restore Service	The average time taken to restore an IT service or other configuration item after a failure. MTRS is measured from when the configuration item fails until it is fully restored and delivering its normal functionality.
Media Gateway Control Protocol	A call control communications protocol used in Voice over IP (VoIP) systems.
Megahertz	One million hertz.

Term	Definition
Memorandum of Understanding	A bilateral or multilateral agreement between two or more parties. It expresses a convergence of will between the parties, indicating an intended common line of action. It is often used in cases where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement.
Memorial Service Network	An organizational unit within the National Cemetery Administration that provides dignified burial and memorial services for eligible Veterans and family members.
Metropolitan Area Network	A large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN
Move, Add, Change, and Disconnect	A request to move, add, change, or disconnect a service.
Multimedia Messaging Service	A standard way to send messages that include multimedia content; e.g., photo, video, audio and text; to and from mobile phones.
National Cemetery Administration	The National Cemetery Administration (NCA) honors Veterans and their families with final resting places in national shrines, and with lasting tributes that commemorate their service and sacrifice to our Nation.
National Change Control Board	The NCCB operates at the Service Delivery and Engineering (SDE) level in the Office of Information and Technology (OI&T), and is responsible for all operations changes. The purpose of the NCCB is to provide leadership and oversight for the National Change Management Process to support change control boards (CCBs) in managing and reviewing national and escalated change requests.
National Electrical Code	National Fire Protection Association (NFPA) Code 70. The National Electrical Code (NEC) provides requirements on electrical wiring and equipment installation issues, including minimum provisions for the use of connections, voltage markings, conductors, and cables.
National Fire Protection Association	An international nonprofit organization whose mission is to reduce the worldwide burden of fire and other hazards on the quality of life by providing and advocating consensus codes and standards, research, training, and education.
National Institute of Standards and Technology	A non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improves quality of life.

Term	Definition
National Service Desk	A single point of contact for all VA IT support; requests, incidents, and problems. Develops and manages a single and consistent suite of IT service management policies, procedures, tools, and technologies used at all levels within VA that are compatible with the IT Infrastructure Library framework.
Network and Security Operations Center	Responsible for protecting VA information on a 24x7 basis; by monitoring, responding to, and reporting cyber threats and vulnerabilities; managing Internet gateways; conducting enterprise-network monitoring; and providing value-added network and security management services as requested.
Network Management System	A system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, SMS or other alarms) in case of outages.
Network Operations Center	One or more locations from which network monitoring and control, or network management, is exercised over a computer, telecommunication, or satellite network.
Next Business Day	The next official working day of the week.
Operations, Maintenance, Administration, Provisioning, and Repair	The collection of functions and processes used to manage an IT system.
Original Equipment Manufacturer	The maker of a final assembly, which may include parts, subsystems, or subassemblies from other companies.
Patient Aligned Care Team	Care coordination by a team, independent of (not always needing face to face) visits.
Personally Identifiable Information	Any information which can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc., alone, or when combined with other personal or identifying information that is linked to a specific individual, such as date and place of birth, mother's maiden name, etc.
Plain Old Telephone Service	Basic telephone service that has been available since the introduction of the public telephone system in the late 19th century.

Term	Definition
Power over Ethernet	A standardized method to pass electrical power along with data on Ethernet cabling. This allows a single cable to provide both data connection and electrical power to devices such as wireless access points, IP telephones, or IP cameras.
Primary Rate Interface	A 1536 Kbps telecommunications interface standard used on an Integrated Services Digital Network (ISDN) for carrying multiple DS0 voice and data transmissions between the network and a user.
Privacy Officer	Responsible for taking proactive measures to help ensure that PII collected by VA is limited to that which is legally authorized and necessary; and is maintained in a manner that precludes unwarranted intrusions upon individual privacy; thereby minimizing privacy events.
Private Switch / Automatic Location Identification	Provides telephone location identification information to the Public Safety Answering Point when a caller using a connecting station of the PBX dials 9-1-1.
Protected Health Information	Individually identifiable health information held by a covered entity or by a business associate acting on its behalf.
Public Safety Answering Point	A call center responsible for answering calls to an emergency telephone number for police, firefighting, and ambulance services.
Public Switched Telephone Network	The aggregate of the world's circuit-switched telephone networks that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication. The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing any telephone in the world to communicate with any other.
Quality of Service	The set of techniques used to manage network resources in order to provide the required level of service.
Recovery Point Objective	The point in time to which data must be recovered after an outage.
Recovery Time Objective	The overall length of time an information system’s components can be in the recovery phase before negatively impacting the organization’s mission or mission/business processes.
Release Package	A set of configuration items that will be built, tested and deployed together as a single release. Each release package will usually include one or more release units.

Term	Definition
Remote Audio Update	Provides the ability to remotely update the audio recording for menus and routing in a menu routing system or interactive voice response system.
Remote Hands Services	Provides local hands, eyes, and ears assistance with maintenance, troubleshooting and installation of hardware and software.
Resource Capacity Management	A process focused on the management of individual components of IT infrastructure; e.g., computer and computer-related equipment, software, licenses, circuits, facilities, or organization (people); through monitoring, measurement, analysis, and reporting.
Risk Management Plan	Documents how risk processes will be carried out during the project.
Service Asset Configuration Management	The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.
Service Capacity Management	The sub-process of capacity management responsible for understanding the performance and capacity of IT services.
Service Desk Manager	An IT service management tool manufactured by Computer Associates.
Service Level Agreement	A negotiated agreement between two parties (i.e., OED and EIE, or OED and FOD) where one is the customer and the other is the service provider. This can be a legally binding formal or informal 'contract' (see internal department relationships). The SLA records a common understanding about services, priorities, responsibilities, guarantees and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service such as billing.
Session Initiation Protocol	A signaling communications protocol, widely used for controlling multimedia communication sessions such as voice and video calls over Internet Protocol (IP) networks.
Short Message Service	A text messaging service that enables devices, such as mobile telephones; to exchange short text messages no longer than 160 alpha-numeric characters and contain no images or graphics.

Term	Definition
Simple Network Management Protocol	An Internet-standard protocol for managing devices on IP networks. Simple Network Management Protocol is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.
System Availability Test	Testing a system against its operational availability requirements.
System Design Document	The System Design Document translates the requirement specifications into a document from which the developers can create the actual system. It identifies the top-level system architecture, and identifies hardware, software, communication, and interface components.
System Engineering Design Review	A solution review performed by Enterprise Systems Engineering.
System Security Plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tabletop Exercise	A tabletop exercise (TTX) involves key personnel discussing hypothetical scenarios in an informal setting. This type of exercise is used to assess the adequacy of plans, policies, procedures, training, resources, and relationships or agreements that guide the prevention of, response to and recovery from a defined incident.
Talent Management System	The single point of access that allows all VA employees and other eligible individuals to manage, select, and record their own training and continuing education.
Technical Reference Model	A framework that categorizes standards and technologies using a common, standardized vocabulary; and provides a foundation of solutions and technologies.
Tier 0 Support	The first level of service provider functions, which is to collect and/or confirm customer and service request information in order to create, prioritize, and assign tickets to appropriate service providers for resolution.
Tier 1 Support	The second level of service provider functions, which include problem screening, definition, and resolution. Service requests that cannot be resolved at this level in a set period of time are elevated to appropriate service providers at the Tier 2 level.

Term	Definition
Tier 2 Support	The third level of service provider functions, which consist primarily of problem identification, diagnosis, and resolution. Service requests that cannot be resolved at the Tier 2 level are typically referred to the Tier 3 for resolution.
Tier 3 Support	The highest level of support. Problem resolution and defect management functions performed at this level usually require specialized resolution.
Time Division Multiplexing	A method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.
Unified Communications	The integration of real-time communication services such as instant messaging (chat), presence information, telephony (including IP telephony), video conferencing, desktop sharing, data sharing (including web connected electronic interactive whiteboards), call control and speech recognition with non-real-time communication services such as unified messaging (integrated voicemail, e-mail, SMS and fax). UC is not necessarily a single product, but a set of products that provides a consistent unified user-interface and user-experience across multiple devices and media-types.
Uninterruptable Power Supply	An electrical apparatus that provides emergency power to a load when the input power source, typically mains power, fails. An uninterruptable power supply differs from an auxiliary or emergency power system or standby generator in that it will provide near-instantaneous protection from input power interruptions, by supplying energy stored in batteries, super capacitors, or flywheels.
Unit Testing	The internal technical and functional testing of a module of code. The developer usually conducts the unit testing.
Version Control System	A system used to manage changes to documents, computer programs, large web sites, and other collections of information.
Very High Frequency	The ITU designation for the range of radio frequency electromagnetic waves from 30 MHz to 300 MHz, with corresponding wavelengths of ten to one meters.

Term	Definition
Video Communications Server	Provides SIP proxy and call control as well as H.323 gatekeeper services for a video communication network; provides connection to video infrastructure, management and endpoint devices; and provides interoperability with Unified Communications, IP telephony networks, and Voice over IP devices.
Virtual Local Area Network	A single layer-2 network that is partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers.
Voice as a Service	A hosted, cloud based, Voice over Internet Protocol telephone service.
Voice over Internet Protocol	A methodology and group of technologies for the delivery of voice communications over Internet Protocol (IP) networks, such as the Internet.
Wide Area Network	A network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, national or international boundaries) using leased telecommunication lines.
Work Breakdown Structure	A deliverable-oriented grouping of project elements that organizes and defines the total scope of the project. Each descending level represents an increasingly detailed definition of a project work.
Workforce Management	Encompasses all the activities needed to maintain a productive workforce.

ADDENDUM F – SECTION C CONTRACT CLAUSES

C.1.0 FSS RFQ INTRODUCTORY LANGUAGE

The terms and conditions of the Contractor's FSS contract (including any contract modifications) apply to all Blanket Purchase Agreements (BPA) and task or delivery orders issued under the contract as a result of this RFQ. When a lower price has been established, or when the delivery terms, FOB terms, or ordering requirements have been modified by the BPA or task/delivery order, those modified terms will apply to all purchases made pursuant to it and take precedence over the FSS contract. Any unique terms and conditions of a BPA or order issued under the contract that are not a part of the applicable FSS contract will govern. In the event of an inconsistency between the terms and conditions of a BPA or task/delivery order and the Contractor's FSS terms, other than those identified above, the terms of the FSS contract will take precedence.

(End of Provision)

C.2.0 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

http://www.acquisition.gov/far/index.html
http://www.va.gov/oamm/oa/ars/policyreg/vaar/index.cfm

(End of Clause)

FAR Number	Title	Date
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	MAY 2011
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT COPYRIGHT INFRINGEMENT	DEC 2007
52.227-19	COMMERCIAL COMPUTER SOFTWARE LICENSE (DEC 2007)	DEC 2007
52.236-7	PERMITS AND RESPONSIBILITIES	NOV 1991
52.237-3	CONTINUITY OF SERVICE	JAN 1991

C.3.0 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (FEB 2012)

(a) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of

the contract, by posting the required information in the Central Contractor Registration database via https://www.acquisition.gov.

(b) As required by section 3010 of the Supplemental Appropriations Act, 2010 (Pub. L. 111-212), all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available. FAPIIS consists of two segments--

(1) The non-public segment, into which Government officials and the Contractor post information, which can only be viewed by--

(i) Government personnel and authorized users performing business on behalf of the Government; or

(ii) The Contractor, when viewing data on itself; and

(2) The publicly-available segment, to which all data in the non-public segment of FAPIS is automatically transferred after a waiting period of 14 calendar days, except for--

(i) Past performance reviews required by subpart 42.15;

(ii) Information that was entered prior to April 15, 2011; or

(iii) Information that is withdrawn during the 14-calendar-day waiting period by the Government official who posted it in accordance with paragraph (c)(1) of this clause.

(c) The Contractor shall receive notification when the Government posts new information to the Contractor's record.

(1) If the Contractor asserts in writing within 7 calendar days, to the Government official who posted the information, that some of the information posted to the nonpublic segment of FAPIIS is covered by a disclosure exemption under the Freedom of Information Act, the Government official who posted the information must within 7 calendar days remove the posting from FAPIIS and resolve the issue in accordance with agency Freedom of Information procedures, prior to reposting the releasable information. The Contractor must cite 52.209-9 and request removal within 7 calendar days of the posting to FAPIIS.

(2) The Contractor will also have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, i.e., for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.

(3) As required by section 3010 of Pub. L. 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

(d) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.

(End of Clause)

C.4.0 52.217-7 OPTION FOR INCREASED QUANTITY--SEPARATELY PRICED LINE ITEM (MAR **1989)**

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting officer may exercise the option by written notice to the Contractor at any time during the contract performance, but in no instance, later than the contract expiration date. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of Clause)

C.5.0 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this Order by written notice to the Contractor at any time during the base period of performance; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least ten (10) days before the Order expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended Order shall be considered to include this option clause.

(c) The total duration of this Order, including the exercise of any options under this clause, shall not exceed twenty- four (24) months.

(End of Clause)

C.6.0 VAAR 852.203-70 COMMERCIAL ADVERTISING (JAN 2008)

The bidder or offeror agrees that if a contract is awarded to him/her, as a result of this solicitation, he/she will not advertise the award of the contract in his/her commercial advertising in such a manner as to state or imply that the Department of Veterans Affairs endorses a product, project or commercial line of endeavor.

(End of Clause)

C.7.0 FAR 52.232-99 PROVIDING ACCELERATED PAYMENT TO SMALL BUSINESS SUBCONTRACTORS (DEVIATION) (AUG 2012)

This clause implements the temporary policy provided by OMB Policy Memorandum M-12-16, Providing Prompt Payment to Small Business Subcontractors, dated July 11, 2012.

(a) Upon receipt of accelerated payments from the Government, the Contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.

(b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns. (c) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

(End of Clause)

C.8.0 VAAR 852.203-71 DISPLAY OF DEPARTMENT OF VETERAN AFFAIRS HOTLINE POSTER (DEC 1992)

(a) Except as provided in paragraph (c) below, the Contractor shall display prominently, in common work areas within business segments performing work under VA contracts, Department of Veterans Affairs Hotline posters prepared by the VA Office of Inspector General.

(b) Department of Veterans Affairs Hotline posters may be obtained from the VA Office of Inspector General (53E), P.O. Box 34647, Washington, DC 20043-4647.

(c) The Contractor need not comply with paragraph (a) above if the Contractor has established a mechanism, such as a hotline, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.

(End of Clause)

C.9.0 VAAR 852.215-70 SERVICE-DISABLED VETERAN-OWNED AND VETERAN-OWNED SMALL BUSINESS EVALUATION FACTORS (DEC 2009)

(a) In an effort to achieve socioeconomic small business goals, depending on the evaluation factors included in the solicitation, VA shall evaluate offerors based on their service-disabled veteran-owned or veteran-owned small business status and their proposed use of eligible service-disabled veteran-owned small businesses and veteran-owned small businesses as subcontractors.

(b) Eligible service-disabled veteran-owned offerors will receive full credit, and offerors qualifying as veteran-owned small businesses will receive partial credit for the Service-Disabled Veteran-Owned and Veteran-owned Small Business Status evaluation factor. To receive credit, an offeror must be registered and verified in Vendor Information Pages (VIP) database. (http://www.VetBiz.gov).

(c) Non-veteran offerors proposing to use service-disabled veteran-owned small businesses or veteran-owned small businesses as subcontractors will receive some consideration under this evaluation factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In addition, the proposed subcontractors must be registered and verified in the VetBiz.gov VIP database (http://www.vetbiz.gov).

(End of Clause)

C.10.0 VAAR 852.215-71 EVALUATION FACTOR COMMITMENTS (DEC 2009)

The offeror agrees, if awarded a contract, to use the service-disabled veteran-owned small businesses or veteran- owned small businesses proposed as subcontractors in accordance with 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors, or to substitute one or more service-disabled veteran-owned small businesses or veteran-owned small businesses for subcontract work of the same or similar value.

(End of Clause)

C.11.0 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

The contracting officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee's authority. A copy of the designation shall be furnished to the Contractor.

(End of Provision)

C.12.0 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

As prescribed in 832.7002-2, insert the following clause: Electronic Submission of Payment Requests (NOV 2012)

(a) Definitions. As used in this clause-

(1) Contract financing payment has the meaning given in FAR 32.001.

(2) Designated agency office has the meaning given in 5 CFR 1315.2(m).

(3) Electronic form means an automated system transmitting information electronically according to the accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, e-mail, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) Invoice payment has the meaning given in FAR 32.001.

(5) Payment request means any request for contract financing payment or invoice payment submitted by the Contractor under this contract.

(b) Electronic Payment Requests. Except as provided in paragraph (e) of this clause, the Contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are considered to be an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) Data Transmission. A Contractor must ensure that the data transmission method and format are through one of the following:

(1) VA’s Electronic Invoice Presentment and Payment System. (See Web site at http://www.fsc.va.gov/einvoice.asp.) (2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI). The X12 EDI Web site (http://www.x12.org) includes additional information on EDI 810 and 811 formats. (d) Invoice requirements. Invoices shall comply with FAR 32.905.

(e) Exceptions. If, based on one of the circumstances below, the contracting officer directs that payment requests be made by mail, the Contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for:

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of clause)

C.13.0 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The Contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/ she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the States of_____. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the Contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

ADDENDUM G – LIST OF ATTACHMENTS

ATTACHMENT 1 - SDE PAO MEETING AGENDA TEMPLATE

SDE PAO Meeting
Agenda Template.doc

ATTACHMENT 2 - SDE PAO MEETING NOTES TEMPLATE

SDE PAO Meeting
Notes Template.docx

ATTACHMENT 3 - VA UC TRM NATIONAL DIAL PLAN

Unified
Communications Natio

ATTACHMENT 4 - EVS POC TECHNICAL SUPPORT TIER MATRIX

EVS Technical
Support Tier Matrix.xls

ATTACHMENT 5 - CONFIGURATION MANAGEMENT PLAN TEMPLATE

Configuration
Management Templat

ATTACHMENT 6 - FIELD OPERATIONS CHANGE MANAGEMENT SOP

FO ChM Process
SOP.pdf

ATTACHMENT 7 - NATIONAL CHANGE PROCESS (NORMAL)

National Change
Process (Normal).pdf

ATTACHMENT 8 - NATIONAL CHANGE PROCESS

National Change Process.pdf

ATTACHMENT 9 - NATIONAL CHANGE PROCESS - PATCHING

National_Change_Process-Patching.pdf

ATTACHMENT 10 - NATIONAL CHANGE MANAGEMENT ESCALATION PROCESS

National Escalation Process.pdf

ATTACHMENT 11 - OIT AVAILABILITY MANAGEMENT PROCESS

oit_availability_management_process_docun

ATTACHMENT 12 - OIT CAPACITY MANAGEMENT PROCESS

oit_capacity_management_process_docum

ATTACHMENT 13 - OIT CHANGE MANAGEMENT PROCESS

oit_change_management_process_documen

ATTACHMENT 14 - OIT CONFIGURATION MANAGEMENT PROCESS

oit_configuration_management_process_dc

ATTACHMENT 15 - OIT EVENT MANAGEMENT PROCESS

oit_event_management_process_document

ATTACHMENT 16 - OIT INCIDENT MANAGEMENT PROCESS

oit_incident_manage
ment_process_docum

ATTACHMENT 17 - OIT KNOWLEDGE MANAGEMENT PROCESS

oit_knowledge_mana
gement_process_docu

ATTACHMENT 18 - OIT PROBLEM MANAGEMENT PROCESS

oit_problem_manage
ment_process_docum

ATTACHMENT 19 - OIT RELEASE MANAGEMENT PROCESS

oit_release_manage
ment_process_docum

ATTACHMENT 20 - OIT REQUEST FULFILLMENT MANAGEMENT PROCESS

oit_request_fulfillmen
t_management_proce

ATTACHMENT 21 - PATCH MANAGEMENT AND COMPLIANCE MEMORANDUM

Patch_Management_a
nd_Compliance.pdf

ATTACHMENT 22 - PATCH MANAGEMENT FLOW CHART

PatchFlowChart.pdf

ATTACHMENT 23 - QUARTERLY CHANGE ORDER REVIEW SOP

Quarterly Review
SOP.pdf

ATTACHMENT 24 - SDE CHANGE MANAGMENT PLAN

National ChM Process SOP.pdf

ATTACHMENT 25 - SDE CHANGE MANAGEMENT PLAN FOR NATIONAL PATCH MGMT

National Patch Management and Chai

ATTACHMENT 26 - SDE NATIONAL CHANGE CONTROL BOARD SOP

NCCB_SOP.pdf

ATTACHMENT 27 - SECURITY IMPACT ANALYSIS TEMPLATE

Security Impact Analysis.pdf

ATTACHMENT 28 - EVS POC CORES (AUSTIN & HINES) INVENTORY LIST

EVS Cores Inventory.pdf

ATTACHMENT 29 - FORT HARRISON INVENTORY LIST

Fort Harrison Inventory.pdf

ATTACHMENT 30 - CONTRACTOR PROJECT MANAGEMENT PLAN TEMPLATE - PENDING

ATTACHMENT 31 - EVS POC SYSTEM SECURITY PLAN - PENDING

ATTACHMENT 32 - EVS HELPDESK PROCEDURE DOCUMENTS - MULTIPLE PENDING

ATTACHMENT 33 - LIST OF NATIONAL VA SUPPORT CONTRACTS - PENDING

ATTACHMENT 34 - SCIENCELOGIC INVENTORY LIST - PENDING

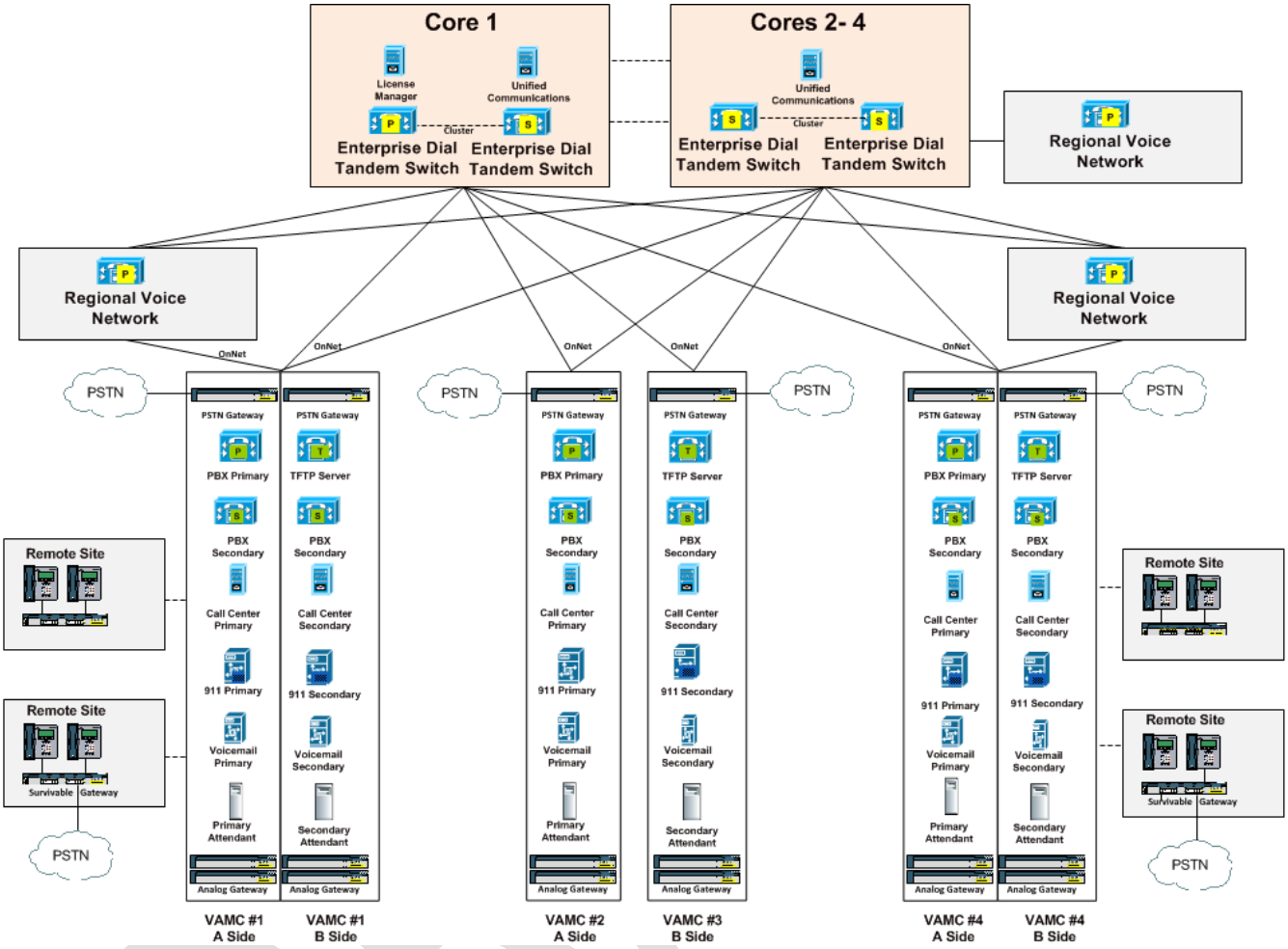
ATTACHMENT 35 - TENNESSEE VALLEY INVENTORY LIST - PENDING

ATTACHMENT 36 - CHARLESTON INVENTORY LIST - PENDING

ADDENDUM H – PoC ARCHITECTURE

The VA EVS PoC system architecture consists of IP-based PBXs installed at each major VA location (e.g. VAMC) with survivable voice gateway equipment at remote sites (e.g. CBOCs, Vet Centers) as depicted in Figure 5.2.1-1 below. The PoC IP based PBXs support multiple open standard voice protocols including SIP, H.323, and MGCP. The IP PBX's are designed in a redundant, high availability configuration. IP based phones are installed at each VA location replacing existing digital and non-compatible IP handsets. IP Phones are connected to VA's LAN infrastructure that supports 802.1af Power over Ethernet (PoE), DHCP, vLANs, and CDP. Patient phones and fax machines that are low cost analog devices require voice gateways for converting to Voice over IP. VA has a variety of fax machines supported by the voice gateways. VA supports a nationwide dial plan that is trunked into VA Core locations using SIP-based tandem switching servers that route on-net calls between VA locations using a hierarchical E.164-based numbering plan. High level system configuration is provided in figure 5.2.1-1, below. Detailed configurations will be provided upon contract award.

Figure H-1



The EVS PoC Architecture consists of component-based voice services, system boundaries, interfaces with existing network connections, and multi-protocol system interactions. Applications, supplies, and services furnished comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp, the Continuous Readiness in Information Security Program (CRISP), including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP).

VMware vCenter Server technology is currently being utilized to manage virtualized hosts and machines in the vSphere virtual infrastructure at VA. The EVS PoC solution utilizes virtualized server technologies with advanced high availability and management support. The virtualized solution provides and enables management operation to be conducted form a single console and to include but not be limited to virtual machine creation, dynamic resource allocation, alerts and notifications, automatic virtual machine failover and automatic host and virtual machine patching and updates. In support of virtualization, all EVS PoC services shall maintain continual accessibility and performance with no degradation during a single point of failure including all administrative access to the system. Each EVS PoC system shall include spare CPU,

memory, and storage capacity to support resource pooling, testing and release management, and increases of system resources on demand. Each EVS PoC system shall support Disaster Recovery capabilities that allow for an entire virtual machine to be restored without manually rebuilding the system. VA maintains CRISP hardware and software release standards that have been tested and verified to meet VA technical and IA guidelines. The Contractor shall provide an EVS PoC lab that mimics the EVS PoC deployment which allows for testing of software and CRISP releases as well as troubleshooting problems.

The following EVS PoC virtualized server features are utilized:

- Virtualized Servers
- High Availability with no single point of failure
- Full administrative access to the system during failure
- Disaster Recovery capabilities
- Backup and Restore capabilities

Additional computing and storage capacity for testing new releases, taking snapshots, testing, with cutover and rollback capabilities

EVS PoC requires multiple integration points for Unified Communications and Information Assurance. The EVS PoC system shall require the following enterprise wide system integration components:

- Active Directory for phone directory and administrative access
- Public Key Infrastructure integration for digital certificates and security
- PIV integration for administrative access
- Additional integration points may be required to meet VA Directives and NIST controls.

EVS PoC system requires complete remote manageability of all system components both through in-band and out of band methods (e.g. KVM) and requires complete visibility into all areas of Fault, Configuration, Performance, Accounting, and Security. EVS PoC will continue to be monitored by the NSOC using existing management tools.