



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

**Office of Information & Technology**

**Managed Contact Center Infrastructure Service**

**Date: 01/19/18**

**TAC-18-xxxxx**

**PWS Version Number: 1.1**

## Contents

1.0	BACKGROUND.....	4
2.0	APPLICABLE DOCUMENTS.....	4
3.0	SCOPE OF WORK.....	8
3.1	ORDER TYPE.....	12
4.0	PERFORMANCE DETAILS.....	12
4.1	PERFORMANCE PERIOD.....	12
4.2	PLACE OF PERFORMANCE.....	12
4.3	TRAVEL.....	12
5.0	SPECIFIC TASKS AND DELIVERABLES.....	12
5.1	PROJECT MANAGEMENT.....	12
5.1.1	OVERALL GOVERNANCE PROGRAM.....	13
5.1.1.1	PROGRAM MANAGEMENT.....	13
5.1.1.2	ESTABLISHMENT OF EXECUTIVE OVERSIGHT COMMITTEE.....	13
5.1.1.3	ESTABLISHMENT OF A MANAGED SERVICES OVERSIGHT COUNCIL.....	14
5.1.1.4	REGULAR MEETINGS AND CONFERENCE CALLS.....	14
5.1.2	REPORTING REQUIREMENTS.....	14
5.1.3	<b>TRANSITION AND TRANSFORMATION (T&amp;T): TRANSITION-IN</b> .....	15
5.1.3.1	T&T: CONTACT CENTER SERVICE PROGRAM.....	15
5.1.3.2	T&T: CONTACT CENTER SERVICE PROGRAM TEAM.....	16
5.1.3.3	T&T: DECISION RIGHTS.....	16
5.1.3.4	T&T: CONTACT CENTER SERVICE PROGRAM PLAN.....	16
5.1.3.5	T&T: CONTACT CENTER SERVICE PROGRAM PLAN PERFORMANCE.....	18
5.1.3.6	T&T: CONTACT CENTER SERVICE PROGRAM REPORTING.....	18
5.2	MANAGED CONTACT CENTER INFRASTRUCTURE SERVICE.....	19
5.2.1	CCS TECHNICAL CAPABILITIES.....	19
5.2.2	CCS MANDATORY FEATURES.....	22
5.3	MANAGED TOLL FREE SERVICES (TFS).....	42
5.3.1	TFS TECHNICAL CAPABILITIES.....	42
5.3.2	MANDATORY TFS FEATURES.....	43
5.4	DISASTER RECOVERY.....	45
5.5	TROUBLESHOOTING AND REPORTING.....	45
5.5.1	TROUBLE TICKET MANAGEMENT.....	46
5.5.2	TROUBLE TICKET MANAGEMENT GENERAL REQUIREMENTS.....	46
5.5.3	REPORTING INFORMATION.....	46
5.6	OPTIONAL TASK ONE – SMALL CONTACT CENTER – MANDATORY SERVICES.....	46
5.7	OPTIONAL TASK TWO – MEDIUM CONTACT CENTER –MANDATORY SERVICES.....	46
5.8	OPTIONAL TASK THREE – LARGE CONTACT CENTER – MANDATORY FEATURES.....	47

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

5.9	OPTIONAL TASK FOUR – CCS OPTIONAL FEATURES .....	47
5.10	OPTIONAL TASK FIVE – TRANSITION OUT .....	63
5.10.1	TRANSITION-OUT TEAM AND REQUIREMENTS PLANNING .....	63
5.10.2	TRANSITION-OUT PLAN .....	63
5.11	OPTION PERIOD .....	65
6.0	GENERAL REQUIREMENTS.....	65
6.1	ENTERPRISE AND IT FRAMEWORK.....	65
6.1.1	ONE-VA TECHNICAL REFERENCE MODEL.....	65
6.1.2	FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM) .....	65
6.1.3	INTERNET PROTOCOL VERSION 6 (IPV6) .....	67
6.1.4	TRUSTED INTERNET CONNECTION (TIC).....	67
6.1.5	STANDARD COMPUTER CONFIGURATION .....	68
6.1.6	VETERAN FOCUSED INTEGRATION PROCESS (VIP) .....	68
6.1.7	PROCESS ASSET LIBRARY (PAL) .....	68
6.2	SECURITY AND PRIVACY REQUIREMENTS .....	69
6.2.1	POSITION/TASK RISK DESIGNATION LEVEL(S) .....	69
6.2.2	CONTRACTOR PERSONNEL SECURITY REQUIREMENTS .....	69
6.3	METHOD AND DISTRIBUTION OF DELIVERABLES .....	71
6.4	PERFORMANCE METRICS .....	71
6.5	SERVICE LEVELS.....	72
6.5.1	SERVICE LEVEL FRAMEWORK.....	72
6.5.2	SERVICE LEVEL REQUIREMENTS.....	74
6.5.2.1	INFRASTRUCTURE SERVICE LEVEL REQUIREMENTS (SLA).....	74
6.5.2.2	OPERATIONAL SERVICE LEVEL REQUIREMENTS (SLA).....	75
6.6	KEY PERSONNEL .....	80
6.7	FACILITY/RESOURCE PROVISIONS .....	80
6.8	GOVERNMENT FURNISHED PROPERTY .....	82
	ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED .....	83
	ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.....	90

## **1.0 BACKGROUND**

The Department of Veterans Affairs (VA) is committed to creating an interactive experience between the Veteran and VA that is easy, pleasant, effective, and personalized. Veterans place more than 140 million phone calls to the VA each year. There are numerous agency phone numbers; there is no roadmap to seamlessly get Veterans the services that they need. VA's contact centers, defined as having two or more individuals answering the phone, has a decentralized, fragmented infrastructure supporting 348 dedicated contact centers. The infrastructure is so fragmented that over 1,000 additional locations are acting as de facto contact centers or performing public outreach duties.. VA owned, operated, and sustained legacy IT systems are expensive to maintain and limit implementation of modern, cost effective systems. Currently, VA cannot realize organizational efficiencies that allow for better first call resolution and the right level of response. Furthermore, VA cannot standardize enterprise efforts for manpower, costs, knowledge and data management. Due to the lack of centralized information, VA senior leadership cannot make strategic decisions on call center improvements. As part of this initiative, VA is looking to transition all its contact centers and associated toll free services to a managed infrastructure service. VA customer contact centers perform all functions associated with receiving and responding to inquiries, and providing information and services through the use of various communications media including, but not limited to, telephones, telecommunications devices for the deaf (TTY), Short Message Service (SMS)/text e-mail, the internet, fax and other media as from a variety of devices (e.g., voice, web, smartphones, mobile devices, etc.). VA's current and planned contact center environment is described in further detail in Attachment A.

VA plans to implement a phased approach to transition its existing contact centers, both within the continental United States (CONUS) and outside CONUS (OCONUS), beginning with a single Veterans Integrated Service Network (VISN). OCONUS locations include Hawaii, Puerto Rico, Guam, US Virgin Islands, and Philippines.

## **2.0 APPLICABLE DOCUMENTS**

In the performance of the tasks associated with this Performance Work Statement (PWS), the Contractor shall comply with the following (**Note:** Most VA-specific documents can be found at <http://www.va.gov/vapubs/>):

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013

7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. 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
9. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
12. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, <http://www.va.gov/vapubs/>
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, <http://www.va.gov/vapubs>
14. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
15. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
17. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
22. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
23. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
24. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)," July 28, 2016
25. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
26. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
27. VA Handbook 6500.6, "Contract Security," March 12, 2010
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
29. OI&T Process Asset Library (PAL), <https://www.va.gov/process/> . Reference Process Maps at <https://www.va.gov/process/maps.asp> and Artifact templates at <https://www.va.gov/process/artifacts.asp>
30. One-VA Technical Reference Model (TRM) (reference at <https://www.va.gov/trm/TRMHomePage.aspx>)

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014
41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
43. 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
44. 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
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

53. 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>)
54. 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>)
55. VA Memorandum "Mandate to meet PIV Requirements for New and Existing Systems" (VAIQ# 7712300), June 30, 2015, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>
56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, [https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC\\_Ref\\_Arch\\_v2-0\\_2013.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf)
57. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
59. 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>)
60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
63. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
64. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
65. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013
66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
69. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
70. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>



- 71. "Veteran Focused Integration Process (VIP) Guide 2.0", May 2017, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>
- 72. "VIP Release Process Guide", Version 1.4, May 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411>
- 73. "POLARIS User Guide", Version 1.2, February 2016, <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412>
- 74. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
- 75. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, <https://www.voa.va.gov/DocumentListPublic.aspx?NodeID=28>
- 76. ATTACHMENT A: Description of Current VA Environment
- 77. ATTACHMENT B: Current Business Environment

### **3.0 SCOPE OF WORK**

The Contractor shall provide a managed contact center infrastructure service solution capable of supporting VA's enterprise-wide call center environment. The managed CCS solution shall be capable of supporting, at a minimum, the current estimated volume of 140 million contacts per year across VA's approximately 9300 agents supporting over 1800 individual contact centers. The managed CCS infrastructure service solution shall support a wide range of customer support work types for all communication channels (e.g., telephone, text, e-mail, WebChat, fax) at an enterprise level. The Contact Center Service (CCS) solution shall integrate all existing VA contact centers, both within the Continental United States (CONUS) and outside CONUS (OCONUS), and shall seamlessly interoperate between all contact centers. The Contractor shall provide the managed infrastructure services on a 24 hour per day, 7 day per week, 365 day per year basis. The managed infrastructure service solution shall include providing toll free services (TFS) into and amongst the contact centers.

The VA's contact center operations currently operate on multiple different platforms with a wide array of capabilities. The scope of this effort shall provide contact center infrastructure that will meet the collective needs of all contact center operations across the VA.

Providing a standardized, single contact center managed service infrastructure capability will facilitate VA contact centers' ability to maximize existing business resources and create an environment for positive veteran experiences.

VA's goal is to transition all of its contact center activities to the managed contact center infrastructure service within 5 years after award of the base contract. The current contact center environment is highly diversified, from medium and large, geographically redundant enterprise-level contact centers (e.g., VBA, VHA Office of Community Care (OCC), VHA Health Resource Center (HRC), VHA Health Eligibility Center (HEC), VHA Veterans Crisis Line (VCL)), that include all of the mandatory features described in 5.2 and most or all of the optional features described in sections 5.9, to small, localized contact centers (e.g., VHA Women Veterans Health, VHA Caregiver Support) which currently leverage telephony solutions with limited functionality (e.g., local VA Medical



## Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Center phone systems). These small contact centers initially require only the mandatory features, but are expected to require optional features to be added, post-migration, as their business processes mature.

Transition of contact centers will be in a phased approach, beginning with a single VISN which includes on average 8-10 VA Medical Centers, to meet VA's identified need to establish streamlined, centralized VISN-level contact center services. These require the mandatory features with the expectation that they will add additional optional features as required. Remaining VISNs will be transitioned following the implementation of the initial VISN.

Additional, small contact centers in operation today may be migrated to the managed infrastructure service simultaneously, requiring the mandatory features with the expectation that they will add additional optional features as required.

VA's medium and large enterprise level contact centers (who require most or all of the mandatory and optional features listed below) require the most extensive planning and coordination. As such, it is expected planning and coordination will begin while VISN transition occurs.

As new contact centers are created, they will be implemented through the managed infrastructure service provided simultaneous with migration activities.

Attachment A includes information describing VA's current infrastructure on which its contact centers operate.

Under the managed services construct, the entire solution (or portions described below) shall be entirely owned by the provider including the infrastructure, code updates, management, change and other necessary practices with the exception of the data. The Government will engage services strictly through outcome based SLAs and rendering of business capabilities presented to the provider.

The Contractor shall provide all management, transportation, equipment, tools, materials, service related equipment (SRE), supplies, installation, supervision, engineering, maintenance, testing, and services necessary to make the circuits, services, functionality, and features fully operational and perform all the tasks associated with providing an enterprise-wide managed contact center infrastructure and associated TFS. The managed infrastructure service shall include ongoing responsibility for 24-hour monitoring, managing and/or problem resolution for the CCS and TFS systems. The Contractor shall be bound by the service-level agreements that state the performance and quality metrics of their relationship, defined in section 6.4. The managed infrastructure services shall not include contact center business operations personnel (e.g., agents). The managed infrastructure services shall be capable of supporting transition of the entire VA enterprise and the remaining VA contact centers are planned to be incorporated following a phased approach. The mandatory features listed in Table 1 are required for all contact centers incorporated into this effort. The optional features listed in Table 2 shall be capable of inclusion to any contact center at the time of migration to the managed infrastructure service or may

## Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

be added at any time to any contact center throughout the period of performance (PoP). The managed CCS infrastructure service shall comply with the Office of Information and Technology (OI&T) Technical Reference Model (One-VA TRM), see section 6.1.1 for further detail.

Contact Center Infrastructure Service Capabilities include the following, not all of which are mandatory:

### Single-Channel (*Individual Licensing*)

### Multi-Channel (*Individual Licensing*)

- SMS Text
- Text Chat (Web Chat)
- E-mail Response Management
- FAX Management
- Web Call Back
- Web Call Through

### Computer Telephony Integration (CTI)

### Collaborative Browsing

### Outbound Dialer

### Intelligent Routing and Call Queuing

- Dialed Number Identification Service (DNIS)
- Automatic Number Identification (ANI)
- North American Numbering Plan (NANP)

### Virtual Queue

### Call Back

### Interactive Voice Response (IVR)

- Self Service
- Speech Recognition
- Automated Call Survey

### Work Force Management

- Forecasting
- Scheduling
- Analytics

### Quality Management

- Call Recording
- Screen Capture
- Monitoring
- Scorecard

## Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

### Supervisor Tools

- Agent and Supervisor Desktop Tools Requirements
- Call Detail Record (CDR)
- Scheduling / Running Reports
- Agent / Supervisor Statistical Data
- Agent Monitoring

### End User Managed Service Platform Training

- Training for Supervisor and Agent application use
- Virtual Training
- Training videos available for AdHoc Training

### Storage

- Application Specific
- Record Specific
- Archive Specific

### Toll Free Service

- Single Number to Call
- Government Service Circuit
- Universal International Toll-Free Number
- Agency-based routing database (also known as Host Connect)
- Alternate Routing (also known as "Cascade" routing)
- ANI Based Routing
- Announced Connect
- Call Redirection
- Service Assurance Routing

### Disaster Recovery/Continuity of Operations

- Disaster Recovery Plan
- Information System Contingency Plan
- Resiliency / Failover
- Continuity of Operations Guide

### Support

- 24x7x365 Support
- Response Times
- Scalability to support 140 million contacts per year minimum, with ability to support additional growth as necessary
- Scalability to support 9300 contact center agents supporting over 1800 individual contact centers, with ability to support additional growth as necessary

The Contractor shall use its own robust telephony (inclusive of voice and IVR services), as well as offer customer services through channels such as email response

management, Short Message Service (SMS), text services and mobile applications, to meet VA's Contact Center requirements.

### **3.1 ORDER TYPE**

Any resultant contract or task order (TO) shall be issued on a firm-fixed price (FFP) basis.

## **4.0 PERFORMANCE DETAILS**

### **4.1 PERFORMANCE PERIOD**

The PoP shall be a five (5) year base period with a one year option period, which may be exercised up to five (5) times, at the Government's discretion. Included are three optional tasks to deploy and sustain managed CCS infrastructure services for additional small, medium and large contact centers across the remaining VA enterprise, which may be exercised numerous times throughout the PoP. Optional task four is for optional managed CCS infrastructure service features, which may be exercised numerous times, at any time throughout the PoP. Optional task five is for 60 days of Transition-out support, which may be exercised one (1) time throughout the PoP.

### **4.2 PLACE OF PERFORMANCE**

Tasks under this PWS shall be performed at Contractor facilities and may also be required in VA facilities located CONUS and OCONUS, as described in section 1, to provide the managed infrastructure services described in this PWS. Work may be performed at remote locations with prior concurrence from the Contracting Officer's Representative (COR).

### **4.3 TRAVEL**

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings throughout the PoP. Travel shall be in accordance with the Federal Travel Regulations (FTR) and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed. Local commuting area is defined as within 50 miles of the location of performance. Include all estimated travel costs in your FFP line items. These costs will not be directly reimbursed by the Government.

## **5.0 SPECIFIC TASKS AND DELIVERABLES**

### **5.1 PROJECT MANAGEMENT**

The Contractor shall provide Project / Program Administrative and Operational support for varying amounts of business and tactical operations for the Onboarding of Contact Centers onto the Managed CCS Infrastructure Services. The Contractor shall provide a Project Management Framework to organize, manage, assess and define, transform and/or install, maintain, and transition the managed call center infrastructure service throughout the Call Center transition. The administrative and operational PM support

shall utilize an industry standard project management framework. The PM support will continue throughout the lifecycle of the contract. The PM Support functions will be to provide guidance, governance, and reporting using Project Management Institute (PMI) framework, while utilizing the Microsoft Word, Excel, PowerPoint, Project, and VISIO tools.

## **5.1.1 OVERALL GOVERNANCE PROGRAM**

### **5.1.1.1 PROGRAM MANAGEMENT**

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

#### **Deliverable:**

- A. Contractor Project Management Plan and updates

### **5.1.1.2 ESTABLISHMENT OF EXECUTIVE OVERSIGHT COMMITTEE**

The Contractor shall appoint members to the Executive Oversight Committee which will be chaired by VA and made up of a number of key executives from the Contractor and VA (inclusive of the Contractor Account Executive), which will meet at a minimum on a quarterly basis, and at such time as its members deem appropriate to perform the following:

- a. Review and analyze the monthly performance reports for the preceding period, including any actual or anticipated budget or schedule overruns, service level attainment of targets, any issues or outages that affect Contractors' overall performance under this TO;
- b. Review progress on the resolution of issues;
- c. Review any requested modifications to the scope of services;
- d. Attempt to resolve, or designate individuals to attempt to resolve, escalated issues; and
- e. Review and attempt to address escalated decisions. Contractor Members of the Executive Oversight Team will include Contractor Account Executive Sponsor, and Contractor Account Executives providing oversight to this TO. The Contractor shall provide to VA for approval an appropriate set of scheduled periodic quarterly meetings or telephone conference calls to be held between representatives from VA and Contractor.

#### **5.1.1.3 ESTABLISHMENT OF A MANAGED SERVICES OVERSIGHT COUNCIL**

The Contractor shall appoint members to the Managed Services Oversight Council which will be chaired by VA Supplier Management Executive and will meet monthly to address business requirements, TO performance, performance standards, continuous improvement, benchmarking, quality assurance and escalated issues and disputes. The Contractor Account Executive providing oversight to this TO will serve as the Contractor's highest ranking representative on such committee and have the authority to commit the Contractor (subject to VA approvals) to implement the course of action as deemed necessary by VA. The Contractor shall provide to the Government for approval an appropriate set of scheduled periodic monthly meetings or telephone conference calls to be held between representatives of VA and the Contractor.

#### **5.1.1.4 REGULAR MEETINGS AND CONFERENCE CALLS**

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

- a. The meetings by the committees noted above; and
- b. Such other meetings of VA and the Contractor personnel, including senior management of the Contractor, as the Government may reasonably request.

For each such meeting, the Contractor shall prepare and distribute an agenda, which will incorporate the topics designated by VA. The Contractor shall distribute the agenda in advance of each meeting so that the meeting participants may prepare for the meeting. In addition, the Contractor shall record and promptly distribute minutes for every meeting for review and approval by VA.

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

#### **Deliverables:**

- A. Executive Oversight Committee Meeting Schedule
- B. Managed Services Oversight Council Meeting Schedule
- C. Meeting Agenda
- D. Meeting Minutes

#### **5.1.2 REPORTING REQUIREMENTS**

The Contractor shall provide the COR with Weekly Progress Reports in electronic form. VA preference for these reports is Microsoft Word and Project formats. The report shall include detailed instructions explanations for each required data element, to ensure that data is accurate and consistent. These reports shall reflect data as of the last day of the preceding week.

The Weekly Progress 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 report shall also include an itemized list of all Electronic and Information Technology (EIT) deliverables and their current Section 508 conformance status. The Contractor shall monitor performance against the CPMP and report any deviations. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

**Deliverable:**

A. Weekly Progress Report

**5.1.3 TRANSITION AND TRANSFORMATION (T&T): TRANSITION-IN**

The Contractor shall have ninety (90) calendar days from TO award to fully setup and operationalize the Services (the T&T activities). The Contractor shall set-up and complete Transition-in to deliver the Services described in this PWS. These initial ninety (90) days will be followed by a thirty (30) day Stabilization period.

**5.1.3.1 T&T: CONTACT CENTER SERVICE PROGRAM**

The Contractor shall designate a resource with the requisite skills and notify the Government of its representative to act as a SPOC the T&T Program (i.e., the T&T Program Manager (PM) / Executive). This person shall be the Contractor representative responsible for program management of the T&T program on an overall basis and shall have primary responsibility for the T&T program management framework. In addition, the Contractor shall initiate T&T (CCS) due diligence activities immediately upon award.

The Contractor shall:

- (a) Define and maintain a standard program charter template for validating and documenting the Transition and Transformation Contact Center Service (TTCCS) Program Plan and associated Integrated Timelines and Heat Maps;
- (b) Define and maintain a standard program management methodology that adheres to best practices;
- (c) Support and assist VA in developing the shared T&T Governance Processes;
- (d) Align the Contractor business and program management processes with the VA T&T organization and T&T Governance Processes;
- (e) Adhere to the T&T program management processes (e.g., T&T Risk / Issue Management, Project Change Requests, etc.);
- (f) Collaborate with VA to identify program reporting requirements;
- (g) Develop standard reporting templates and processes to track program progress that facilitates summarizing information;



- (h) Deploy the standard reporting templates to facilitate monthly reporting to management
- (i) Monitor Contractor performance at a T&T program level;
- (j) Provide assistance in reviewing and resolving T&T program level Issues;
- (k) Report and track the status of critical deliverables and milestones across the T&T Program; and
- (l) Provide VA with the relevant and timely information and documentation to review and confirm completion of each T&T deliverable and milestone.

The Contractor shall conduct, within seven (7) days after award, a Kick-off Workshop with all stakeholders to develop the high-level TTCCS Program Charter to include program objectives, scope, schedules, and stakeholder roles and responsibilities. The Contractor shall present, for review and approval by the Government, the details of the intended approach, Program Plan, and Project schedule for the Transition-in. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least two (2) calendar days prior to the meeting), and meeting minutes (shall be provided to all attendees within three (3) calendar days after the meeting). The Contractor shall invite the CO, Contract Specialist (CS), COR, the VA PM, and others as requested by VA.

**Deliverable:**

- A. TTCCS Program Charter

**5.1.3.2 T&T: CONTACT CENTER SERVICE PROGRAM TEAM**

The Contractor will staff and onboard its TTCCS Program team no later than five (5) calendar days after award.

**5.1.3.3 T&T: DECISION RIGHTS**

A decision rights model shall also be finalized by the VA T&T Governance organization, in collaboration with the Contractor within the fifteen (15) Business Days after award. The decision rights model will facilitate decision-making relative to the Transition-in, as it pertains to the VA stakeholders, the VA T&T Governance organization, Contractor, and other potential third parties. The model will focus on “who makes a decision”, “who facilitates the decision”, and “who participates in the decision”. The final model implemented will be the result of collaboration between the Contractor and VA. The decision rights model will be delivered with the TTCCS Program Plan.

**5.1.3.4 T&T: CONTACT CENTER SERVICE PROGRAM PLAN**

The Contractor shall develop and submit the TTCCS Program Plan that identifies all the tasks to be undertaken to perform the requisite Transition-in, the completion date for each task, the assignment of responsibilities between VA and the Contractor, and any special resources to be provided by the Contractor, VA or third parties. The TTCCS Program Plan shall also set forth the Contractor’s approach, timeline, and tools to be used in execution of the Transition-in. The TTCCS Program Plan shall take the form of both a narrative and graphic format that displays the schedule, milestones, risks, and

resource support. In addition, the TTCCS Program Plan shall include how the Contractor will coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the TTCCS program period. The initial baseline Program Plan shall be concurred upon and updated in accordance with Section B of the TO. The Contractor shall update and maintain the VA approved TTCCS Program Plan through the Transition-in and Stabilization periods. The TTCCS Program Plan shall also state the goals of each stage of the Transition-in. For clarity, the Contractor shall develop, maintain and execute the TTCCS Program Plan.

The TTCCS Program Plan shall include:

- The overall approach including, but not limited to, technology implementation and set-up Governance, including roles and responsibilities.
- Kick-off workshop results and actions
- Sample workflow of all voice and data processes and exchanges
- The key activities and operating results
- The acceptance criteria linked to such results
- The data for the stages linked to such results
- An outline of how the Contractor intends to work with VA to ensure an orderly collection of the knowledge base / scripts for the Services
- Requirements for collaboration with VA to ensure proper set-up of the Services
- Set-up and onboarding management including, roles and responsibilities of the Contractor for the set-up and onboarding period
- Clearly defined estimate of Contractor's, VA's, and third parties' resources required to complete the tasks
- Information on activities to interface with the VA ITSM Tool and any other tools that are included in the Contractor solution platform
- Identification of risks, risk minimization strategies, and preventive measures
- A plan for Contractor's staff onboarding and location(s) from where the Services will be performed
- A plan for technology implementation
- A plan for the communications implementation (including ACD, IVR, etc.)
- A plan to configure and populate the knowledge management System and knowledge base
- A plan to collect existing knowledge base scripts from VA
- Location setup plan
- FAQ Service implementation plan
- Plan to establish Governance for the Services
- A list of planned, routine, and ad hoc data collection reports including frequency and formats
- Steady-State Account Team organizational chart (with named resources)

- Steady-State Governance Account Team roles and responsibilities
- An Availability plan detailing reactive (monitoring, measuring, analysis, and management of Events, Incidents, and Problems involving Service outages) and proactive (proactive planning, design, recommendation, and improvement of Availability) activities for the Contractor's Services infrastructure and Systems.

**Deliverable:**

A. TTCCS Program Plan

**5.1.3.5 T&T: CONTACT CENTER SERVICE PROGRAM PLAN PERFORMANCE**

The Contractor shall perform the Services described in the TTCCS Program Plan in accordance with the schedule set forth therein. The Contractor shall perform each of the Transition-in Services in a manner that will not unnecessarily disrupt the business or operations of VA or unnecessarily degrade the Services than being received by VA from existing internal or external providers.

Prior to undertaking any Transition-in activity, the Contractor shall identify all known material risks and shall not proceed with such activity until VA approves the plans with regard to such risks provided, however, that, neither Contractor's disclosure of any such risks to VA, nor VA's acquiescence in Contractor's plans, shall operate or be construed as limiting Contractor's responsibilities under this PWS. The TTCCS Program Plan shall group transition activities and deliverables by Transition phases. The Contractor shall not proceed to the next phase until (i) all transition activities and deliverables associated with the preceding phase have been completed by Contractor and accepted by VA and (ii) VA has expressly authorized the Contractor to proceed to the next phase. The Contractor shall identify and resolve, with VA's reasonable assistance, any problems that may impede or delay the timely completion of each activity or deliverable in the TTCCS Program Plan that is the Contractor's responsibility, and shall use all commercially reasonable efforts to assist VA with the resolution of any problems that may impede or delay the timely completion of each task in the TTCCS Program Plan that is VA's responsibility. The Contractor shall provide all cooperation and assistance required by VA in connection with VA's evaluation or testing of the activities and deliverables set forth in the TTCCS Program Plan.

**5.1.3.6 T&T: CONTACT CENTER SERVICE PROGRAM REPORTING**

The Contractor shall conduct weekly status reviews and provide VA with a written status report describing accomplishments, progress against the TTCCS Program Plan, next week's activities, issues, risks, and risk mitigation approaches until Transition-in has been successfully completed. The Contractor shall provide oral reports more frequently if reasonably requested by VA. The Contractor shall conduct status and issue meetings more frequently as needed with impacted stakeholders across the VA. Promptly upon receiving any information indicating that Contractor may not perform its responsibilities or meet the timetable set forth in the TTCCS Program Plan, the Contractor shall notify VA in writing and shall identify for VA's consideration and approval, specific measures to address such delay and mitigate the risks associated therewith.

The Contractor shall conduct a review with all participating stakeholders within ten (10) calendar days after Services go-live to create a Lessons Learned Report for future managed services transition initiatives

The Contractor shall provide the TTCCS Status Report utilizing the agreed Transition-in templates to report progress to management. The report shall include a description of accomplishments and progress against the TTCCS Program Plan, including next week's activities, issues, risks and risk mitigation approaches.

The Contractor shall provide a monthly TTCCS Service Level Implementation Report detailing progress on implementing the Service Levels as part of Transition-in and Stabilization

**Deliverables:**

- A. TTCCS Status Report
- B. Lessons Learned Report
- C. TTCCS Service Level Implementation Report

## **5.2 MANAGED CONTACT CENTER INFRASTRUCTURE SERVICE**

The Contractor shall provide a managed CCS infrastructure solution which provides services and infrastructure to enable VA to deliver customer service to the Veteran across multiple contact channels (e.g., voice, fax, email, Internet web site, SMS, chat) by providing a single or multiple call queues. The network call queue shall manage multimedia customer interactions such as voice, email, web submissions, and fax. The call queue(s) shall provide consistent, real-time management and distribution of multi-media calls to the contact center. The managed CCS infrastructure solution shall include associated TFS to facilitate external and internal communications.

### **5.2.1 CCS TECHNICAL CAPABILITIES**

The Contractor shall provide a fully managed CCS infrastructure service solution, complete with SRE and enterprise-quality communications tools. The CCS solution shall be designed and configured by the Contractor, and shall be fully compatible with VA's core enterprise voice systems (e.g., voice, fax, email, website, etc.) and supporting infrastructure. The Contractor shall:

1. Ensure the managed CCS infrastructure solution is completely implemented and ready for full operation within 90 days from the contract award date. The Contractor shall ensure minimum disruption to current VA operations. The deployment and transition to the managed CCS infrastructure service solution shall be seamless and transparent to the calling public.
2. Provide recommendations to identify any prioritize CCS locations and supplementary services (e.g., existing toll free numbers) that may need to be transitioned before others. The Contractor shall provide a fully functional and tested managed CCS infrastructure service prior to transitioning any existing VA sites, to minimize disruptions. It is critical to provide VA customers with the same

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

high level of service when they are calling into VA's main toll-free number throughout all transition and implementation activities.

3. The Contractor shall include all activities and costs required to transition the current VA call center services to the proposed managed infrastructure service solution in a Detailed Project Plan.
  - a. The Contractor shall delineate and identify in the plan roles and responsibilities for VA, the contractor, and any third party vendors required to transition the existing contact center service to the Contractor's managed service solution.
  - b. The plan shall include any labor requirements, SRE, facilities requirements, and hardware/software requirements needed to fully implement the proposed solution.

The Contractor shall provide call management services as part of its managed CCS infrastructure solution, including:

1. The capability for a network call queue (a single queue or multiple queues according to VA needs) to manage the routing and distribution of contacts from multi-media channels such as voice, text, chat, email, facsimile, and VA web sites.
2. The intelligent routing and distribution of contacts according to the real time operating status of the VA contact center(s) and its business rules, such as media type, real time status of the contact center, caller profile, call content, and agent skills. The contractor shall provide the capability to prioritize queues and contacts within a queue.
3. The CCS shall interoperate with the VA's CCS communications channels such as the web site, e-mail, voice, fax and chat (when applicable).
4. The CCS shall have the capability to traverse and successfully interoperate with VA firewalls and security layers. The contractor shall verify with VA that VA's firewall is compatible with the service.
5. The CCS call management solution shall support service observation, which provides VA authorized personnel with the capability to monitor the CCS trunks, agents, and agent groups for call quality. The contractor shall provide options for silent monitoring (default) and three-way audio conferencing. Service observation shall be made available for monitoring both local and remote agents and support local and remote observers. Service observation shall be secured in accordance with VA security requirements and available only to authorized VA-designated individuals.
6. The Contractor shall provide VA with the capability to manage its specific network queue, call routing algorithms, contact center agent profiles, and reports. The CCS shall enable authorized VA designated individuals to perform both real time and scheduled changes. The CCS management system shall provide the following minimum administrative capabilities:
  - a. An audit trail and change log history

- b. Authentication IAW VA requirements (e.g., PIV)
  - c. Ability to perform scheduled and real-time changes
  - d. Ability to view the VA CCS configuration
7. The Contractor shall provide VA with access to graphical, real time reporting of the CCS queue status. The real time reporting shall monitor performance and identify all interactions (e.g., voice, email, fax, web, chat) by contact channel and agent status. The reports shall include summaries and totals (where applicable). The real time reporting shall provide the following minimum capabilities:
- a. Number of inbound contacts, broken out by contact type
  - b. Status of inbound contacts
  - c. Number of contacts in queue
  - d. Length of oldest contact in queue
  - e. Average queue time
  - f. Number of abandon contacts
  - g. Agent status and performance statistics
  - h. Service level information
  - i. Number of contacts handled by workgroup or skill
8. The CCS shall provide the capability to inform the caller of the queue status including the callers estimated wait time in queue when a queue threshold exceeds an agency defined threshold. This shall also include an option for announcing the caller's expected wait time. The CCS shall provide the ability to change recorded announcements.
9. The CCS shall provide the capability to transmit and deliver music on hold (or recordings) to the originating caller. The music on hold source can be contractor or VA provided.
10. The CCS shall supply terminal devices (e.g., phones, IP phones, softphones) required for delivery of CCS if requested by VA. Terminals shall have the capability to support caller ID and an optional name/message display (where applicable).
11. The Contractor shall be responsible for the purchase, installation, de-installation, and maintenance and support of all SRE required to support the managed CCS solution, including TFS. The SRE to be provided by the contractor shall be new and not refurbished.
12. The CCS shall provide the capability to accommodate VA contact center closings (e.g., scheduled holidays, unplanned closings, outside of normal business hours, and closings for maintenance activities) by providing announcements, messages, or re-routing of contacts during the period when the VA contact center is closed.

The managed CCS infrastructure service solution shall support and manage multimedia customer interactions such as voice, text, chat, email, web submissions, and fax while eliminating the need for hardware, software, training and maintenance and other type of costs normally associated with in-house CCS infrastructure.

The Contractor's managed CCS infrastructure solution and architecture shall encompass all components, systems, and applications required to maintain and track calls from the Internet and Public Switched Telephone Network (PSTN) using the underlying access and transport service(s). The contractor shall meet the requirements for interfaces to deliver customer service capabilities, through intelligent routing, to the endpoint call center agent workstation and/or to the subsequent call transfers. The design shall include support and interoperability with VA existing applications. The contractor shall provide a detailed architecture and design showing the CCS capability to interoperate with the VA environment, see Attachment A. The managed CCS infrastructure solution shall not rely on the use of any government furnished property (GFP) to connect the public (or VA customers) to an answering site.

**Deliverable:**

- A. Detailed Project Plan
- B. Detailed Architecture and Design Plan

**5.2.2 CCS MANDATORY FEATURES**

The contractor's proposed managed infrastructure service offering shall include the standard features listed below for all contact centers. Further detail on each feature is provided in Table 1.

- a. Intelligent Routing and Call Cueing
- b. Interactive Voice Response (IVR)
- c. Quality Management
- d. Call Recording and Monitoring
- e. Storage Requirements
- f. Agent Features
- g. End-User Managed Service Platform Training
- h. Supervisor Tools
- i. Agent and Supervisor Desktop Tools

These mandatory features shall be included for all contact centers as they are migrated to the managed infrastructure service.

**TABLE 1: MANDATORY FEATURES**

Mandatory CCS Feature	Technical Requirements	Business Requirements
-----------------------	------------------------	-----------------------



Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
Intelligent Routing and Call Queuing	<p>Provide queues for combinations of provider skills and contact modalities of voice, chat, web, <u>etc.</u>, through which agents will be presented a contact based on business rules and assigned skills.</p> <p>The ability to route to the appropriate agent based on time of day, agent availability, skill, preferred language, and agent priority queue or a combination of these variables.</p> <p>Call transfer and conference capabilities for the agents. Warm call transfer capabilities for the agents. The ability to directly transfer the caller unassisted allowing the agent to release from the call. This shall provide a solution that will apply internal and external transfers for inbound and/or outbound calls. The CCS shall provide conference call capabilities for the agents. The CCS shall provide the ability to place a caller on hold, add additional parties into the call. This shall apply for internal and external calls, both inbound and/or outbound calls. The CCS shall provide the capability to transfer to a queue or a specific agent. The CCS shall provide the capability to place multiple parties on hold allowing the agent to toggle between callers. The CCS shall provide feedback to the representative with a ring tone during a transfer.</p> <p>The CCS shall provide the ability to place a caller on hold, add additional parties into the call, and transfer the caller to added party. This shall apply for internal and external transfers for inbound and/or outbound calls.</p> <p>The CCS shall be capable of integration with Workforce Management tools and software. The CCS shall provide the supervisor with the ability to log off agents or change agent state. The CCS shall provide alternative routing for routing services failure (default routing on premise). The CCS shall provide the identity of the number that was dialed or the web site from which the contact is initiated in order to direct the contact to the right contact center or organization. The CCS shall recognize the contact method and distribute the contact per the contact type (i.e. a chat</p>	<p>Ability to communicate to the caller the expected waiting time</p> <p>Ability to communicate to the caller their position in the queue</p> <p>Ability to play music to callers while on hold</p> <p>Ability to select/manage the music being played to the callers while on hold</p> <p>Ability to play music to callers in a queue</p> <p>Ability to select/manage the music being played to the callers in a queue</p> <p>Ability to identify and prioritize callers based on configured business rules</p> <p>Ability to manage callers in a queue</p> <p>Ability to prescreen a caller before routing to a queue</p> <p>Ability to have multiple queues based on skill base, IVR selection, Priority etc.</p> <p>Ability to have enterprise queues</p> <p>Need the ability to Configure customer message for blocked calls</p> <p>Need the ability to play a customer message for blocked calls</p> <p>Need the ability to configure routing rules for individual caller</p> <p>Need the ability to transfer a</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>request to an agent who is skilled to handle a chat). The CCS shall determine the right agent at the right center to whom the contact shall be forwarded to provide best possible treatment and shortest wait time. The CCS solution shall determine whether the call should get IVR treatment based on the number that was dialed and route to call to the right IVR and the right application.</p>	<p>call into a Call Queue</p> <p>Need the ability to transfer a call to a known available Agent (warm transfer option)</p> <p>Need the ability to have "in queue" announcement capability</p> <p>Call delivery based on real time availability / wait time</p> <p>Need the ability to route a call using parameters such as skill, level of expertise, etc.</p> <p>Need the ability to route a call to a level of skill based queue (novice, intermediate, expert)</p> <p>Need the ability to have the ability to route based on attributes</p> <p>Need the ability to configure the system to route to idle agents based on skill</p> <p>Need the ability to route calls to any available agent when an agent with the needed skill is not available</p> <p>Need the ability to configure the system to route based on time of day, day of week, etc.</p> <p>Blind routing (e.g. hunt groups without agent status) for emergencies. Need the ability to have blind routing capability. Need the ability to configure the blind routing rules.</p> <p>Need the ability to configure call routing using prioritization rules</p> <p>Need the ability to move priority</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>based calls ahead in the queue</p> <p>Need the ability to test routing configurations using routing simulation</p> <p>Need the ability to have call tracing capability</p> <p>Need the ability to configure text routing based on business rules (number, type (new, reply))</p> <p>Need the ability to route texts by TBD business rules</p> <p>Ability to pull chat from the queue</p> <p>Engage and disengage overflows</p> <p>On demand message recording, turn on / off</p> <p>Ability to define hours of operation, including holidays, weekends, special days, etc.</p> <p>Emergency message on / off</p> <p>Remote emergency condition on / off</p> <p>Emergency overflow on / off</p> <p>Emergency queue flush</p> <p>System is capable to assign, report, and modify multiple skill groups within a call center. Administration and Reports for multiple can be handled same as single.</p> <p>Ability for overflow of call activity from one queue to another based on configurable</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>thresholds.</p> <p>Ability to route based on the caller's phone number, IVR entries, or other caller attributes.</p> <p>Ability to Route a call that either does not have normal routing or loses routing plans, due to system glitch. Also known as default routing.</p> <p>Ability to assign queues with higher / lower priority over others to determine service levels per queue.</p> <p>Ability for a Chat Agent to pull from more than one queue. Local queue and Centralized queue as example.</p> <p>The call routing/queueing shall have the ability use business rules for call handling settings by team (e.g., hold thresholds, ACW time, auto answer).</p> <p>Ability to configure call workflows per call type. Screen pops for one call type; longer after call work on other call type; auto answer; service levels; etc - all configurable by call type</p>
Interactive Voice Response (IVR)	<p>The contractor shall provide an interactive voice response application that allows callers to be provided with information based upon input from (a) telephone DTMF key pad entries or via (b) speech recognition. The minimum capabilities are listed below:</p> <ol style="list-style-type: none"> <li>1. The IVR solution shall select pre-recorded announcement messages with the capability for announcements and provide the ability for a caller to opt out during an announcement to a predefined termination. Such announcements shall always be played from the beginning for each caller and provide</li> </ol>	<p>Need the ability for customers to initiate all voice contact with the VA through one 1 800 number ("The Single Front Door")</p> <p>Ability to have one ""Front Door"" enterprise level IVR interaction to service all callers</p> <p>Ability to set an initial greeting per number</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>the capability to be recorded in U.S. English.</p> <p>2. The CCS shall provide the ability to leave caller information via telephone DTMF keypad signal or speech (e.g., name, address, account information, etc.).</p> <p>3. The CCS solution shall allow agents and supervisors to retrieve caller-entered DTMF or speech messages.</p> <p>4. For transcription of caller information, the IVR shall provide (a) transmission of the recorded voice files and DTMF data for each call to the agency and (b) a report of caller responses that transcribes the caller-provided information for the ordering agency based upon the agency's needs and transmits it to the agency. The IVR shall provide transcription reports from English.</p> <p>5. The IVR solution shall query a database that delivers agency-provided information to the caller. The database may be housed in the (a) ordering agency or, at the ordering agency's discretion, (b) housed in a contractor location and updated by the ordering agency.</p> <p>6. The IVR solution shall provide a default routing or message if the database is unavailable.</p> <p>7. The IVR shall allow callers to hear and verify their names and addresses in an agency-provided name and address database after the caller has entered his or her telephone number via DTMF, or based on the caller's ANI. (Text to Speech).</p> <p>8. The IVR shall support speech recognition as a valid caller input.</p> <p>9. The IVR shall support at a minimum, all spoken numeric digits as well as "yes" and "no."</p> <p>10. The IVR shall accept and process at a minimum 95 percent of the above speech responses. The speech responses which are not accepted shall be routed to default location designated by the ordering agency.</p> <p>11. The IVR shall provide the capability to perform surveys (via DTMF or speech) to IVR callers. The surveys can be provided to all or a random percentage of callers according to agency needs. Survey results shall be provided electronically to VA.</p> <p>12. The IVR shall provide a facsimile "fax back" capability (Fax or equivalent) that shall permit callers to retrieve agency-specific documents or forms. The IVR</p>	<p>Ability to set an initial greeting per set of numbers</p> <p>Ability to have an announcement capability for different classes such as General, Emergency etc.</p> <p>Ability during an emergency to flush and end all calls in a queue</p> <p>Ability to shut down a call center using graceful shutdown approach</p> <p>Ability for a customer or agent to access an extension directory</p> <p>Ability to provide multiple modes of IVR navigation such as DTMF menu/ Basic, guided, Speech</p> <p>Call segmentation capability to (DTMF menu/ Basic, guided, Speech)</p> <p>Call segmentation - basic speech (press or say)</p> <p>Ability to offer transaction Services through the IVR Self-Serve option (for example address change, Phone number change)</p> <p>Ability to identify callers during the IVR phase (e.g., through database interaction)</p> <p>Ability to authenticate a Caller prior to offering any Self-Serve transactional services</p> <p>As an IVR user need the ability to manage routing rules by individual caller</p> <p>As an Admin I need the ability to manage (Add, Change Delete etc. ) routing rules</p> <p>Need the ability for an Admin to</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>shall fax back the request documents within one hour of the initial call and retry a minimum of 13 attempts over a six-hour interval to complete the request. Fax transmittal shall include an option for a cover sheet (standard or customized).</p> <p>13. At VA's option, the IVR shall provide a solution that will allow the caller's selection(s) information shall be transferred to the VA.</p> <p>14. The contractor's IVR capacity must be configured such that the application answers a call within 3 ring cycles for 99 % of the offered call volume (measured on an hourly basis).</p> <p>15. The IVR shall allow features equivalent to the above shall be available to individuals who are hearing impaired or have speech disabilities via electronic means in Baudot and ASCII/TTY code formats. These electronic form lines need not be voice feature enabled.</p> <p>16. The IVR shall provide summary reporting that at a minimum provides information on the caller, average call duration, caller opt out (transfer) and disposition of the calls within The IVR solution application on a daily, weekly and monthly basis.</p> <p>17. The IVR shall provide the ability to route calls or provide information based upon a database query(s) of information provided by a database located at the ordering agency premises. The query(s) could be to single, redundant, or multiple databases depending upon agency specifications and the complexity of the application. The contractor shall implement and provide the appropriate interface and connectivity for the contractor's IVR application to successfully query and access VA's database(s). The IVR solution caller shall have the capability to retrieve, review, and modify information located on the agency based database based upon the agency's needs. The agency database(s) can be a (a) mainframe or (b) server based relational database. If the database does not respond to the network query within 250 milliseconds, a VA defined default routing plan shall be used.</p> <p>18. The IVR shall provide natural speech recognition for IVR applications with the ability, at a minimum, to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, alpha numeric numbers. At a minimum, the contractor shall provide natural speech recognition</p>	<p>customize IVR messages by Enterprise, Line of Business and by Customer Class</p> <p>Need the ability to classify a call based on customers IVR selections</p> <p>Need the ability to classify a call in real time</p> <p>Need the ability to classify a call based on information collected by the system (i.e. IVR)</p> <p>Need the ability to classify a call based on historical data</p> <p>Need the ability to prioritize calls based on caller history or caller status. Much like a "Gold" Member club treatment.</p>



Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>capabilities and vocabularies for English (American). The minimum accuracy threshold for speech recognition shall provide be at least 95%.</p> <p>19. The contractor shall make available any IVR reports that are available with its equivalent commercial offerings.</p> <p>20. The IVR shall be able to recognize alphabet, numbers, and basic speech for all calls.</p> <p>21. The IVR shall provide the ability to make run time configuration changes to the script and phone tree.</p> <p>22. The IVR shall provide the user to navigate up the phone tree and/or skip to different branches of the phone tree.</p> <p>23. The IVR shall support configurable time-out to allow for transfer.</p> <p>24. The IVR shall integrate to RDBMS databases via SQL.</p> <p>25. The IVR shall provide VA the ability to access all data captured by solution.</p> <p>26. The IVR solution &amp; applications manager shall provide the ability to view a caller's real-time activity and progress for troubleshooting and reporting purposes.</p> <p>27. The IVR solution shall support call volumes as defined.</p> <p>28. The IVR solution shall provide the ability to stop or change a message immediately or at a predetermined time.</p> <p>29. The IVR shall provide an application to manage and record voice messages.</p> <p>30. The IVR shall provide an application to allow the integration of voice messages to the phone tree.</p> <p>31. The IVR solution shall provide a solution that will compare an entered value to a database value from databases or other data sources IVR is connected to.</p> <p>32. IVR solution shall provide a separate:</p> <ul style="list-style-type: none"> <li>• Production Platform</li> <li>• Development and Pre-Production platform</li> </ul> <p>33. The IVR solution shall provide capable to access information in an external database and speak that</p>	



Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>value.</p> <p>34. The IVR solution shall provide prompt for input and act on responses.</p> <p>35. The IVR solution shall accept the calling party number (CPN) from the caller, and have the ability to use this to access information in the database, and forward this information to the screen pop on the desktop.</p> <p>36. The IVR solution design provided shall be 508 compliant for all internal and external customers.</p> <p>37. The IVR solution shall provide users the access to IVR Self Service options 24 hours, 7 days a week if configured for self-service options.</p> <p>38. The IVR solution shall provide reporting, summarizing, and reviewing IVR statistics for each contact center (examples that shall provide be included as a minimum are below):</p> <ul style="list-style-type: none"> <li>• Number of calls received</li> <li>• Number of callers entering The IVR solution</li> </ul> <p>39. The IVR solution shall provide a solution that will show average duration of all calls while traversing</p> <p>40. The contractor shall provide an IVR solution that will provide a measurement of caller activity by use of check points or call flow points</p> <p>41. The IVR shall provide the number of callers using each menu option</p> <p>42. The IVR shall provide the number of callers opting out and at what point in the application</p> <p>43. The IVR shall provide IVR availability statistics</p> <p>44. The IVR solution shall provide Remote Audio Update (RAU) capabilities for disaster/emergency needs and messages to The IVR solution menus in real time.</p> <p>45. The IVR solution shall provide the ability to transfer calls back to ACD.</p>	
Quality Management	<p>Digital recording and monitoring of inbound and outgoing multimedia contacts (telephone, email, and web self-service channels) and associated data (agent screen capture) to capture the caller experience. At a minimum, the date, time, duration, caller ID information (if</p>	<p>Ability to create sample / retrieve based on call parameters</p> <p>Ability to pull from sample</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>available), dialogue, and identity of the agent handling the call shall provide be captured and recorded. Archived calls shall be able to be retrieved by date, time, agent, content, contact channel, or identity of the caller.</p> <p>Tools for call tracing, validations, training, and compliance. The contractor shall provide voice recording initiation based on activity (active recording or event driven recording). The contractor shall comply with FIPS Publication 140-2, "Security Requirements For Cryptographic Modules".</p> <p>Capability for the recording of an agent to be activated and de-activated on demand.</p> <p>Remote monitoring and playback</p> <p>Reporting (management and administrative)</p> <p>Programmable scheduled and random call recording</p> <p>Selective recording (based on business rules)</p> <p>Support free seating</p> <p>Total and random recording of all calls</p> <p>Convert call recordings to .wav or mp3 file format</p> <p>Ability to develop QM forms for quality monitoring and provide capability for multiple scoring systems and provide the ability to evaluate and score calls when performing random quality reviews. The call recording solution shall provide reports for the following requirements:</p> <p>Calls shall be tracked by ACD group, work unit, and individual agent. The contractor shall provide the ability to sort and report the data.</p> <p>Call shall be date and time stamped.</p> <p>The agent shall provide the ability to randomly select calls for quality review. The contractor shall provide note when the call is reviewed and by whom. The review of the call shall be associated with the recording of the call.</p> <p>All completed call reviews shall be stored and can be sorted in the same manner as recorded calls.</p> <p>The Quality Management solution shall provide reports</p>	<p>Ability to push from sample to reviewer</p> <p>Embedded scorecard</p> <p>Scorecard review workflow</p> <p>Custom templates for quality evaluation scorecard</p> <p>Ability to attach Notes / recording attachment to the quality evaluation scorecard</p> <p>Export to file / email for scorecard</p> <p>Reporting</p> <p>Translation of recording</p> <p>Ability to transcribe calls</p> <p>Ability to Search</p> <p>Ability to attach files to call recordings such as external eval, supervisory note, email correspondence, text, picture (e.g., screen capture), etc</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>hourly, daily, weekly, monthly and annually. A variety of recording reports shall be available, by agent, by team, by evaluator, by form, and by graded call count.</p> <p>The Quality Assurance solution shall provide the ability to pause a live or recorded screen capture and print the screen.</p> <p>Secure storage for voice calls and screen capture 100% call recording for Agents Screen capture of 20% of recorded calls and will include ability to record dual monitors. Capability for the supervisor to monitor in real time with screen capture and voice. Capability to adjust the screen capture percentage at the agent level. Solution for voice and screens shall record all segments of a call (e.g. agent to caller, agent to supervisor, agent, caller and supervisor, agent to another queue). Meet FIPS 140-2 encryption in transit and at rest for all call recorded voice and screen data services. The ability to search and monitor calls using at least 5 search criteria to include at least: CPN, agent name/number, screen capture present, call length, and team designations. Provide the ability to utilize the QA form without having to link it to a call. The ability to search for graded calls by date, time, and agent name/number, evaluator, team, and station number. The ability to manually start a recording at any point during a call by either agent or supervisor. Speech analytics of the recorded calls, automatic methods of analyzing speech to extract useful information about the speech content. Voice recording based on schedules. The ability to capture 100 percent of voice traffic. The ability for the administrators/supervisors to manually delete Personally Identifiable Information (PII). Capability of synchronizing audio and screen recordings. The ability for the administrator/supervisor to listen to stored audio recordings 100 percent of the time. The ability to announce to the caller that the call is being recorded. The ability for the administrator/supervisor to replay stored call and screen recordings. The ability for the administrator/supervisor to have a live</p>	

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>recording of a conversation sent to his/her mailbox. The ability for the administrator/supervisor to flag recordings for complaints or threats. The ability to include caller detail information along with the recording. The capability to monitor in real time with screen capture and voice. The capability to record both inbound and outbound calls. The capability to perform recordings for Quality Management (QM) which can be selected randomly or targeted for evaluation for quality of service.</p>	
Call Recording and Monitoring	<p>The managed service solution shall provide digital recording and monitoring of inbound and outgoing multimedia contacts (telephone, email, and web self-service channels) and associated data (agent screen capture) to capture the caller experience. At a minimum, the date, time, duration, caller ID information (if available), dialogue, and identity of the agent handling the call shall be captured and recorded. Archived calls shall be able to be retrieved by date, time, agent, content, contact channel, or identity of the caller. Call recordings shall be stored according to the storage requirements section. The following minimum capabilities shall be provided:</p> <ul style="list-style-type: none"> <li>Archive recordings</li> <li>Playback of recording</li> <li>Provide the capability for the recording of an agent to be activated and de-activated on demand.</li> <li>Remote monitoring and playback</li> <li>Reporting (management and administrative)</li> <li>Programmable scheduled and random call recording</li> <li>Selective recording (based on business rules)</li> <li>Support free seating</li> <li>Total and random recording of all calls</li> <li>Convert call recordings to .wav or mp3 file format</li> <li>The call monitoring system shall also provide the capability for evaluating and scoring calls and performing random call quality reviews.</li> </ul> <p>The contractor shall provide seamless integration with agent recording and monitoring.</p>	<p>Ability to access to recordings</p> <p>Ability to share recordings</p> <p>Ability to Screen capture</p> <p>Ability to mark recording - call parameters</p> <p>Ability to mark recording - CTI Data</p> <p>Ability to capture chat 100% of chat scripts</p> <p>Ability to search recordings</p> <p>On demand recording</p> <p>Need the ability to mask out PII (e.g., credit card information when taking a payment over the phone).</p> <p>Ability to save recorded file locally</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements																		
Storage Requirements	<p>Storage capability shall be provided to meet 100% call recording/20% screen capture (if used) and allow 15-month online retrieval capability, with records greater than 15 months in age archived. Storage shall meet requirements set forth by National Archives and Retention Authority (NARA), specifically as follows:</p> <table data-bbox="418 514 1157 1024"> <tr> <th>Subject Matter Area</th><th>Disposition Authority Number</th><th>Retention Requirement</th></tr> <tr> <td>Crisis Line Records</td><td>DAA-0015-2017-0001-0001</td><td>Destroy 4 year(s) after cutoff</td></tr> <tr> <td>Medical Advice</td><td>DAA-0015-2017-0001-0002</td><td>Destroy 4 year(s) after cutoff</td></tr> <tr> <td>Benefits</td><td>DAA-0015-2017-0001-0003</td><td>Destroy no sooner than 6 year(s) after cutoff but longer retention is authorized</td></tr> <tr> <td>Detailed Administration Information</td><td>DAA-0015-2017-0001-0004</td><td>Destroy 2 year(s) after cutoff</td></tr> <tr> <td>Routine Administrative Information</td><td>DAA-0015-2017-0001-0005</td><td>Destroy 7-30 days depending on business need of the organization</td></tr> </table>	Subject Matter Area	Disposition Authority Number	Retention Requirement	Crisis Line Records	DAA-0015-2017-0001-0001	Destroy 4 year(s) after cutoff	Medical Advice	DAA-0015-2017-0001-0002	Destroy 4 year(s) after cutoff	Benefits	DAA-0015-2017-0001-0003	Destroy no sooner than 6 year(s) after cutoff but longer retention is authorized	Detailed Administration Information	DAA-0015-2017-0001-0004	Destroy 2 year(s) after cutoff	Routine Administrative Information	DAA-0015-2017-0001-0005	Destroy 7-30 days depending on business need of the organization	
Subject Matter Area	Disposition Authority Number	Retention Requirement																		
Crisis Line Records	DAA-0015-2017-0001-0001	Destroy 4 year(s) after cutoff																		
Medical Advice	DAA-0015-2017-0001-0002	Destroy 4 year(s) after cutoff																		
Benefits	DAA-0015-2017-0001-0003	Destroy no sooner than 6 year(s) after cutoff but longer retention is authorized																		
Detailed Administration Information	DAA-0015-2017-0001-0004	Destroy 2 year(s) after cutoff																		
Routine Administrative Information	DAA-0015-2017-0001-0005	Destroy 7-30 days depending on business need of the organization																		
Agent Features		<p>Need the ability to dial a toll free Direct Access number</p> <p>Need the ability for Agents to be contacted from a Direct Access number</p> <p>Need the ability to dial a local Direct Access number</p> <p>Ability to make an outbound call via desk phone or soft phone to pay line, international and toll free numbers</p> <p>Need ability for an agent to transfer a call to a toll free Backend access number</p> <p>Need the ability to transfer a call to a local Backend access number</p> <p>Need the ability to view in real</p>																		

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>time calls that are being blocked</p> <p>Need the ability for an Agent use either a soft phone or desktop landline to support customers</p> <p>to provide the user with normal call control operations (answer, hold, retrieve etc.)</p> <p>Need the ability for an Agent to build a personal phone book/personal transfer list / phone book</p> <p>Need the ability to provide the Agent with a department (call center) phone book – dial</p> <p>Need the ability to provide the user with a global (Agency) phone book – dial</p> <p>Need the ability to provide the user with a global transfer list / phone book</p> <p>Need the ability for an agent to change their availability</p> <p>Need the ability for an Agent to set a reason code when they are wrapping up a call</p> <p>Need the ability for an Agent to set a reason code when not in ready state</p> <p>Need the ability to display Agents Productivity statistics on the Agents Desktop</p> <p>Need the ability to view my current</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>personal performance Need the ability to view my daily personal performance</p> <p>Customizable templates – end user Ability to add some custom buttons for call control options if needed. In addition to hold, mute, transfer, etc - adding buttons for special treatment options or handling. (custom buttons)</p> <p>Need the ability for an Agent to have voice mail capability Some call center agents have voicemail, as they get queued calls as well as direct to extension calls from the IVRs. Direct calls can get voicemail.</p> <p>Need the ability to provide the Agent with call data such as IVR selections, time in queue, etc. - Data shows on the agent desktop tool</p>
End User Managed Service Platform Training	<ol style="list-style-type: none"> <li>1. The Contractor shall provide training that encompasses all systems installed under the tasks in the PWS.</li> <li>2. Scheduling of the training curriculum shall be subject to an agreement between the Contractor and the Government based on the deployment schedule.</li> <li>3. All instruction shall be provided by qualified instructors of the systems installed.</li> <li>4. Depending on the type of user training, the Contractor shall provide all attendees with the</li> </ol>	



Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>appropriate training materials, to include manuals, text materials and course curriculum necessary for the specific training.</p> <ol style="list-style-type: none"> <li>5. The course curriculum shall be subject to review and approval by the Government prior to commencement of the training.</li> <li>6. The Contractor shall provide, approved by the Government, virtual interactive training, for all business end users.</li> <li>7. For future training purposes, the Contractor shall provide, Government approved, recorded training media, of all systems installed, with the capability to chat/help line for further instruction, for the purpose of questions that may arise during video training. The recordings shall encompass each category for all systems.</li> <li>8. The Contractor shall provide training sufficient to provide introductory and intermediate operation of the systems.</li> </ol>	
Supervisor Tools	<p>Supervisor Tools shall be provided for use by supervisors of different levels and by agent team leads to observe group status and manage daily operations of assigned groups, teams or agents.</p> <p>Required functions include:</p> <p>On-demand monitoring and recording tools:            Shall provide at a glance current status of all agents a supervisor is responsible for with breakdown by teams            Supervisor shall be able to select any agent from the list to receive detailed status            Supervisor shall be able to engage silent monitoring and selective recording. Supervisor presence must not be reflected as a conference call and must not affect agent ability to control call, including ability to initiate and complete transfer            Supervisor shall have ability to save recording as a file and use it for training, reviews or disciplinary actions            Supervisor shall have ability to barge in or completely intercept call if necessary            Supervisor shall be able to receive alerts for pre-defined events (e.g. log in, exceeded time in not ready state,</p>	<p>Manual traffic redirect            Skill assignment override</p> <p>Consolidated skill group / expression status and statistics view - real time</p> <p>Consolidated reporting (cross time zone included)</p> <p>Need the ability to generate reports for interactions across all channels</p> <p>Need the ability to generate a report with the breakdown for all contacts received through all channels</p> <p>Need the ability to view interactions across all channels and modalities in an executive dashboard</p> <p>Need the ability to manage the</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
	<p>etc.)</p> <p>Call assistance and escalation handling tools:</p> <p>Supervisor shall be able to set availability for assistance and escalation calls visible for agents</p> <p>Supervisor shall be notified about assistance or escalation requests and able to see type of request</p> <p>System shall maintain reports showing number and timing of escalations and assistance calls with breakdown per supervisor and agent</p> <p>Supervisor shall have ability to log a note or select assistance/escalation reason</p>	<p>reason codes</p> <p>Need the ability for a Manager to view Agent Teams Productivity statistics</p> <p>Need the ability to view my group's/team's daily performance</p> <p>Need the ability to request assistance</p> <p>Need the ability to add a 3rd party to a direct conference a lead</p> <p>Need the ability to escalate a call/chat to an escalation queue</p> <p>Team status at glance</p> <p>Forced agent state changes</p> <p>Team members re-assignment</p> <p>Ability to chat with team member(s) and record chat.</p> <p>Ability for supervisor send a blast/broadcast message</p> <p>Silent monitoring Barge in</p> <p>Whisper used by supervisors to speak to agents without caller hearing</p> <p>Call Intercept (Taking over the call (not 3 way))</p> <p>Assign temporary skill Move to different skill group Change skill grade/level View staffing by skill</p> <p>Provide count, time and</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>percentage type of statistics</p> <p>Agent statistics to present totals, max / min and averages</p> <p>Group statistics to present totals, max / min and averages</p> <p>Pre-defined views (templates)</p> <p>Customizable templates – administrator</p> <p>Real-time Reporting: Report objects – tables, graphs, drop down lists</p> <p>Real-time Reporting: Filters based on call data and agent events</p> <p>Real-time Reporting: Configurable thresholds and alarms (color, sound, email)</p> <p>Real-time Reporting: Report Refresh rate</p> <p>Real-time Reporting: Configurable reported object selection</p> <p>Real-time and Historical Reporting:</p> <p>Provide access restrictions per reporting objects</p> <p>Scheduled reports</p> <p>Reports should be available for data no longer than 5 minutes after data event</p> <p>Reports should take no longer than 5 minutes to run.</p>

Managed Contact Center Infrastructure Service  
TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>Reporting Aggregation (5 minutes, 30 minutes, 60 minutes)</p> <p>Direct data access (including export in different formats)</p> <p>Custom templates</p> <p>Provide count, time and percentage type</p> <p>Individual statistics to present totals, max / min and averages</p> <p>Group statistics to present totals, max / min and averages</p> <p>Pre-defined views (templates)</p> <p>Customizable templates – administrator</p> <p>Provide access restrictions per object and views</p> <p>Scheduling of reports</p> <p>Call Detail Records: Full cross component call detail records Attached call data availability Timing of non-call activities as relates to call processing</p> <p>Ability to have broadcast message or text to play on agent desktops to alert to current issues / status.</p> <p>Ability to see a selected agent's statistics for period of review</p> <p>Reports show in tabular or grid or graphic format</p> <p>Report parameters selectable via drop down lists</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Mandatory CCS Feature	Technical Requirements	Business Requirements
		<p>Reports allowing drill downs or expanded views as desired. Example - show Team stats, and drop down to see all agents.</p> <p>Preferred report access via a web client.</p> <p>Call Detail Records (e.g., start, queue, agent, extension, duration, who hung up, and any GUID used by system / carrier) to resolve manager or customer inquiries related to individual calls.</p> <p>Ability for call center activity to be communicated to 3rd party system (e.g., readerboards) to show real time data using industry interfaces (e.g., APIs).</p>
Agent and Supervisor Desktop Tools Requirements	<p>Desktop tools will provide information on current and historical states</p> <p>Desktop softphone must provide following functions and features:</p> <p>Normal call control operations (e.g., answer, hold, retrieve)</p> <p>Phone book for manual dial out</p> <p>Agent state change buttons</p> <p>Reason code for time in wrap up state</p> <p>Reason code for time in not ready state</p> <p>Multiple line appearance (private extension)</p> <p>performance statistics (real time and cumulative from the beginning of the day / shift)</p> <p>group / team and queues stats – current</p> <p>Desktop software must provide following functions and features for managers Team and individual status at glance</p> <p>Forced agent state changes</p> <p>Real time team member queue re-assignment</p>	

### **5.3 MANAGED TOLL FREE SERVICES (TFS)**

VA uses TFS to support the inbound voice service which provides a toll free number (no charge to caller) access to the managed CCS infrastructure service solution described above. The Contractor's managed CCS infrastructure solution shall include a managed TFS component, which shall connect to and interoperate with the PSTN and VA's CCS agents.

#### **5.3.1 TFS TECHNICAL CAPABILITIES**

The Contractor's managed TFS capabilities shall include the following:

1. The Contractor shall act as the responsible organization or "Resp Org" for assignment and maintenance of toll-free numbers if requested by the ordering agency.
2. The Contractor shall ensure the TFS is provided as a Government service circuit so it cannot be disconnected.
3. The Contractor shall support toll-free number portability.
4. The Contractor shall provide, manage and maintain TFS into the managed CCS infrastructure service solution described above. Average call volume across all VA Toll Free numbers is provided in the table below.
5. The Contractor shall offer Universal International Toll-Free Number service (also known as Universal International Free Phone Number - UIFN). This UIFN shall enable VA to request a single, unique toll-free number that is the same throughout the world (where available commercially from participating countries), to include domestic and international TFS with nationwide single number coverage and call routing features (e.g., area code routing, time of day and day of week routing, percent allocation routing, alternative routing)
6. The Contractor shall ensure the TFS allows for a single toll-free number to terminate at multiple service delivery points (SDPs) and multiple toll-free numbers to terminate at a single location (SDP).
7. As a default measure, the TFS shall provide a busy signal or recorded announcement for all calls that encounter network congestion and/or terminating egress congestion, as determined by VA.
8. The TFS shall provide a network intercept to record announcements as an inherent network capability when a call cannot be completed. At a minimum, such generic announcements shall be provided for the following conditions:
  - a) Time out during dialing
  - b) Denial of access to features and other related conditions
  - c) Denial of access to non-domestic or restricted calls

## Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

9. The TFS shall provide customized network intercept recorded announcements. The contractor shall provide options for the custom announcement to be a) recorded by the contractor or b) recorded remotely by VA.
10. The TFS shall, at a minimum, provide all announcements recorded in English. Other languages shall be optional.
11. The TFS shall provide Dialed Number Identification Service (DNIS). DNIS will enable multiple toll-free numbers to be routed and uniquely identified on a shared trunk group. The TFS shall transmit DNIS digits, upon VA request, prior to the delivery of a TFS call to uniquely identify the dialed toll-free number. The DNIS digit length shall be 10 digits.
12. The TFS shall identify and provide the calling parties Automatic Number Identification (ANI) to assist VA with identifying malicious or emergency calls.
13. U.S. and Canadian callers shall be able to reach VA using TFS Numbers linked to the VA's existing local telephone number (switched access) or a dedicated nodal circuit.
14. Non-domestic callers in other countries shall be able to call using International TFS Numbers, making it easy for global customers to reach and access VA's customer service centers in the U.S.
15. Using TFS Inbound, calls shall be routed to the managed CCS infrastructure service to deliver seamless 24-hour, around-the-clock support.
16. The Contractor shall include all necessary service-related equipment (SRE), including terminal devices and software, to provide the managed TFS.

### VA Contact Center Toll Free Service

#### Total Domestic & international (Approximate)

Approximate Number of Minutes
140 Million per year (average 5 to 10 min per call)

### 5.3.2 MANDATORY TFS FEATURES

The Contractor's proposed managed TFS offering shall include the standard features listed below to be included for all contact centers. These mandatory features shall be included for all contact centers as they are migrated to the managed infrastructure service.

Name of Feature	Description
-----------------	-------------

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Name of Feature	Description
Agency-based routing database (also known as Host Connect)	The Contractor shall provide routing of TFS calls with associated data based upon a query(s) of information provided by a database located at VA premises. The query(s) could be to single, redundant, or multiple databases, depending upon agency specifications and the complexity of the application.
Alternate Routing (also known as "Cascade" routing)	The TFS shall allow calls to be re-routed on a pre-determined plan based upon availability of trunks (busy) at the terminating location, a maximum number of calls allowed in progress, or a pre-defined ring-no-answer condition. If none of the alternate terminations are able to receive the call, then the call shall be terminated to (1) a predefined announcement, or (2) a busy signal, at VA's option.
ANI	Automatic Number Identification (ANI). The TFS shall allow transmission of the caller's real time ANI information (full 10 digit number or non-domestic equivalent) to the ordering agency.
ANI Based Routing	The TFS shall enable calls to be routed based upon the originating ANI of the caller. Default routing defined by VA shall be used if ANI is not available.
Announced Connect	The TFS shall provide a customized message to the called party, before the caller is connected, and provide the called party with information about the caller (e.g. ANI, account number etc.). This feature is commonly referred to as a "whisper."
Call Redirection	<p>The TFS shall enable calls to be transferred by the Contractor's network, no matter which platform the call is being re-directed from, from the called party/agent to another toll-free number or any PSTN number by using, at VA's discretion, any one of the three following modes of network level call transfer:</p> <ol style="list-style-type: none"> <li>1. Blind transfer (unsupervised)</li> <li>2. Verification by the agent and then transfer (supervised)</li> <li>3. Three-way conference and then transfer</li> </ol> <p>The Contractor shall ensure that there is no double billing for toll free calls that have been transferred using call redirection. This includes calls redirected within the contractor's network from one operating platform to another operating platform.</p>
Service Assurance	The TFS shall route calls to an announcement or a predefined



Name of Feature	Description
Routing	alternate termination within five minutes of the agency request if an emergency situation or service disruption occurs. The TFS shall complete routing requests to other types of terminations within thirty minutes of the request.

#### **5.4 DISASTER RECOVERY**

The Contractor shall ensure that disaster recovery (DR) procedures are engaged once any critical functionality has been non-operational for two (2) hours. The Contractor shall provide a Disaster Recovery Plan that outlines all triggers, thresholds, and events associated with DR engagement, including steps to invoke DR and steps to return to normal operation. The Contractor shall provide an Information System Contingency Plan that contains procedures and technical measures that enable the recovery of the system, business operations, and data. The plan shall provide necessary steps to be taken when expected normal operational or DR operational procedures or outcomes are circumvented by events. All procedures and technical measures in the Contingency Plan shall be included in the Master Test Plan and tested as a part of the Authority to Operate (ATO) effort before the system is placed in production to ensure that contingency actions will work when needed. The Contractor shall provide a Continuity of Operations Guide that outlines all steps that will be followed in the event a disaster interrupts business to ensure that essential functions will continue to be performed.

##### **Deliverables:**

- A. Disaster Recovery Plan
- B. Information System Contingency Plan
- C. Continuity of Operation Guide

#### **5.5 TROUBLESHOOTING AND REPORTING**

The Contractor shall provide tools to allow detailed reporting to track the provided managed contact center infrastructure and toll free services. The reporting tool shall be web-based and intuitive, secure, and reliable. The report tool shall allow users to select the reporting time period(s) and allow for flexible delivery options (on demand or scheduled for future delivery).

The Contractor shall provide an online reporting tool that allows for different delivery formats (via web, email or download) and allows users to schedule for future delivery. The reports that VA needs to view and access will be used to identify and/or validate trends and patterns in call traffic, volume of calls, usage analysis for billing, SLA performance, and other reporting elements needed to gauge the health and status of the quality of service provided by the managed service provider.

### **5.5.1 TROUBLE TICKET MANAGEMENT**

The Contractor shall perform trouble ticket management in accordance with commercial best practices, and shall meet the government's requirements specified below.

### **5.5.2 TROUBLE TICKET MANAGEMENT GENERAL REQUIREMENTS**

The Contractor shall create a trouble ticket for any reported and discovered service issues, provide status updates, provide online real-time access to trouble ticketing and system status information, update open trouble tickets and escalate as needed, and report the resolution to the initiator. The Contractor shall establish and implement procedures and systems for 24x7x365 trouble ticket and complaint collection, entry, tracking, analysis, priority classification, and escalation for all services to ensure that problems are resolved within the timeframes specified in Section 6.4 Service Levels. The Contractor's ticket system shall ensure data transparency with/between its system and VA's existing ServiceNow™ ticketing system. The Contractor shall ensure VA has read-only access to the ticketing system dashboard. As the first priority, the Contractor shall restore any Telecommunication Service Priority (TSP) restoration coded service, as quickly as possible, using best effort. The Contractor shall escalate issues according to the CPMP.

### **5.5.3 REPORTING INFORMATION**

The Contractor shall provide the Government with the capability to query, sort, export, and save in formats such as PDF/CSV or standard/structured file formats trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record. The Contractor shall process any credits applicable to the service outage based on this record of information. SLAs and credits are defined in Section 6.4 Service Levels. The Contractor shall, upon request from VA, deliver archived trouble and complaint report data within five (5) days of the request for such information

## **5.6 OPTIONAL TASK ONE – SMALL CONTACT CENTER – MANDATORY SERVICES**

The Contractor shall implement a small VA contact center into its managed contact center infrastructure service solution. The managed infrastructure service shall include all the mandatory functions, features, and services described in sections 5.1, 5.2, 5.3, 5.4, and 5.5 of this PWS. A small contact center is generally described as a limited, regional coverage and which typically handles contact volumes of less than 5000 per day with less than 100 agents. Further details on the existing environment is provided in Attachment A.

## **5.7 OPTIONAL TASK TWO – MEDIUM CONTACT CENTER –MANDATORY SERVICES**

The Contractor shall implement a medium VA contact center into its managed contact center infrastructure service solution. The managed infrastructure service shall include all the mandatory functions, features, and services described in sections 5.1, 5.2, 5.3, 5.4, and 5.5 of this PWS. A medium contact center is generally described as a limited,

regional (e.g., VISN-level) contact center, which may support 8-10 sites (e.g., VAMCs) and which typically handles contact volumes of 15,000 per day across approximately 300 agents. Further details on the existing environment is provided in Attachment A.

## **5.8 OPTIONAL TASK THREE – LARGE CONTACT CENTER – MANDATORY FEATURES**

The Contractor shall implement a large VA contact center into its managed contact center infrastructure service solution. The managed infrastructure service shall include all the mandatory functions, features, and services described in sections 5.1, 5.2, 5.3, 5.4, and 5.5 of this PWS. A large contact center is described as a contact center which typically handles contact volumes in excess of 15,000 calls per day with over 300 agents. Further details on the existing environment is provided in Attachment A.

## **5.9 OPTIONAL TASK FOUR – CCS OPTIONAL FEATURES**

If exercised by VA, the Contractor shall include any single, multiple, or all features listed below to its managed CCS infrastructure service solution to any VA contact center receiving service under this effort. Optional features may be included at time of implementation of the VA contact center or at any time during the PoP after implementation. Details on which optional features shall be included will be specified in the individual TOs. For each optional feature ordered for an existing contact center, implementation shall be completed within 3 months of order.

The contractor shall provide the following optional managed service offerings as for any contact center. Further detail on each feature is provided in Table 2.

- a. IVR (Spanish)
- b. IVR (Advanced Speech Capabilities and Analytics)
- c. Collaborative Browsing
- d. Computer Telephony Integration (CTI)
- e. E-Mail Response Management
- f. Outbound Dialer
- g. Text (SMS)
- h. Text Chat (Web Chat)
- i. Text Chat (Web Chat) – Additional Capabilities
- j. FAX Management
- k. Web Call Back
- l. Web Call Through
- m. Workforce Management
- n. Virtual Queue
- o. Automated Call Survey
- p. Metrics Storage Requirements

**TABLE 2: CCS OPTIONAL FEATURES**

Optional CCS Feature	Custom Requirements	Business Requirements
----------------------	---------------------	-----------------------

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

IVR (Spanish)	<p>The IVR shall provide natural speech recognition, for Spanish, for IVR applications with the ability, at a minimum, to recognize spoken vocabulary, digits, zip codes, credit card numbers, credit card expiration date, account numbers, alpha numeric numbers.</p> <p>The IVR solution shall select pre-recorded announcement messages with the capability for announcements and provide the ability for a caller to opt out during an announcement to a predefined termination. Such announcements shall always be played from the beginning for each caller and provide the capability to be recorded in Spanish (American).</p> <p>At a minimum, the IVR shall provide natural speech recognition capabilities and vocabularies for Spanish (American) dialects. The minimum accuracy threshold for speech recognition shall provide be at least 95%.</p> <p>The IVR shall be capable of transcription of caller information from Spanish, the contractor shall provide (a) transmission of the recorded voice files and DTMF data for each call to the agency and (b) a report of caller responses that transcribes the caller-provided information for the ordering agency based upon the agency's needs and transmits it to the agency. The contractor shall provide transcription reports for Spanish-speaking callers.</p> <p>The IVR shall provide support, all spoken numeric digits as well as "yes" and "no." in Spanish.</p>	<p>Need the ability for the IVR to support multiple languages (English and Spanish)</p> <p>Need the ability to translate Spanish.</p>
IVR (Advanced Speech Capabilities & Analytics)		<p>Need the ability for customers to navigate the IVR using natural speech</p> <p>Need the ability to have natural speech call segmentation capability</p> <p>Voice analytics - 100% of the calls</p> <p>Voice analytics configuration</p>
Collaborative Browsing	<p>The CCS shall allow bi-directional sharing of web pages between the contract center agent and the caller. It shall enable a caller to request a co-browse session with a contact center agent. The agent shall have the capability to highlight text and scroll the browser screen to a specific section of a web page. The agent shall have the capability to push a web page to the caller and vice-versa. The CCS shall allow</p>	<p>Ability to offer collaboration session via chat or voice call</p> <p>Ability to initiate session via button</p> <p>Ability to initiate session via link (sent by agent when on the phone)</p> <p>Ability to request and receive an</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>the capability for an agent to transfer control of a collaborative browsing session to another agent and log all collaborative interactions between the agent and caller. The contractor shall state if there are any restrictions or limitations regarding the type of web browser software used by the caller or contact center agent for use with this feature. The CCS shall provide the ability to mask fields and inputs of private/sensitive information.</p> <p>Must meet Federal and VA security requirements.</p>	<p>explicit customer permission to initiate session</p> <p>Ability to immediately disconnect session upon customer disconnect</p> <p>Ability to push Web Content thru multiple channels (e.g., text, e-mail)</p> <p>Ability to provide assistance with Forms and Templates</p> <p>Ability to allow Follow me browsing" option to help customer</p> <p>Ability to capture and report session / pages visited</p>
Computer Telephony Integration (CTI)	<p>The CCS shall provide Computer Telephony Integration (CTI) capability to enable transfer of caller information and agency specified data between the contractor and agency specified systems simultaneously with the associated inbound contact channel (call). This feature is used to support a diverse set of agency applications such as screen pop/splash, intelligent routing, third party call control, keyboard dialing, enhanced reporting, and multi-channel call blending solutions.</p>	<p>Need the ability to display caller and call history information to the Agent when the call is routed to the Agent</p> <p>Need ability for agent desktop to provide a screen pop based on caller events / input by interfacing with third party applications via industry standard APIs</p>
E-mail Response Management	<p>The CCS shall provide E-mail Response Management (ERM) that shall assign a tracking ID to each email and route e-mail communication according to agency specified business rules. The ERM shall provide the following minimum capabilities:</p> <p>Auto response</p> <p>Automatic acknowledgement</p> <p>Email classification and prioritization</p> <p>Email routing (omni-queue) based upon business rules</p> <p>Filtering capability</p> <p>Content analysis and knowledge base for suggested and personalized responses</p> <p>Management reports</p> <p>Real time exception reports</p> <p>The ERM shall be compatible with the ordering agency's e-mail application.</p>	<p>Monitored email box with published (web, paper mail, phone) email address</p> <p>Route email based on address used</p> <p>Ability to configure email routing business rules</p> <p>Ability to Classify email based on destination address</p> <p>Ability to configure email classification business rules</p> <p>Ability to Classify email based on subject line</p> <p>Ability to Classify email based on parsed email content</p> <p>Ability to Push email to agent</p> <p>Ability to notify users on pending</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

		<p>mail/responses</p> <p>Allow agent to pull email from queue</p> <p>Send receipt / confirmation back with generic SLA</p> <p>Send receipt / confirmation back with SLA based on subject line or parsed text</p> <p>Ability to auto respond to sender (based on type assigned)</p> <p>Ability to select from a pre-set templates to respond to a Veteran/sender</p> <p>Ability to provide each agent a personalized/custom template</p> <p>Ability to generate reports on email handling</p> <p>Ability to analyze email text for historical analysis</p> <p>Email statistics and analytics</p>
Outbound Dialer	<p>The contractor shall provide automated outbound dialing and provide function to design, organize, and manage outbound campaigns. The dialer service shall support either centralized or distributed contact center environments according to the ordering agency's needs. The dialer shall have the following minimum capabilities:</p> <p>Automatically initiate domestic and non-domestic outbound calls</p> <p>Call conferencing and call transfer capability</p> <p>The system shall have the tools and technology to allow the execution of outbound campaigns in predictive and preview modes. Predictive dialing - capture real-time statistics from the call queue and automatically adjusting the outbound dialing frequency according to agency defined service level parameters. Preview dialing - allow agents to preview the customer record before an outbound call is initiated and provide an option for the agent to cancel the call</p> <p>Receive and manage inbound calls</p> <p>Support agent blending. The integration of outbound and inbound call handling to determine how to best use agent resources. (agents can handle both outbound and inbound calls)</p> <p>Support service observation</p> <p>The system shall be able to create campaigns from existing data source(s) based on rules defined by a</p>	<p><b>OUTBOUND CALLING</b></p> <p>Ability to make an outbound call to pay line, international, and toll free numbers</p> <p>Ability to configure the number appearing on the called party caller ID</p> <p><b>OUTBOUND CAMPAIGN</b></p> <p>Ability to create outbound campaign lists from VA data sources using industry standard interfaces (e.g., API, import)</p> <p>Ability to configure the outbound campaign(s) using business rules such as, # of attempts, leaving VM, flag bad numbers and no connect numbers</p> <p>Ability to create dial lists for outbound campaigns</p> <p>Ability to configure the dialing times for outbound campaign based on time zones</p> <p>Ability to generate an outbound campaign list for manual calling</p> <p>Ability to have preview dialing for outbound campaigns</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>user, build associated dialing list based on contact information available for customer, and prepare to be dialed either sequentially by system or by agent or team assignment.</p> <p>The Outbound Campaign Solution shall create and manage campaigns list from an external data source. Outbound campaigns must take into consideration customer's location and time zone to avoid making calls early mornings or late nights.</p> <p>The Outbound Call Campaign solution shall comply with information provided in the National No-Call List. The system campaign management platform shall be able to comply with the applicable laws of each state or municipality related to outbound dialing such as do-not-call lists. There are federal and state level legislation that govern outbound dialing.</p> <p>The Outbound Call Campaign solution shall adjust the time of the call based on the receiver's time zone. This is to ensure that the VA complies with calling window laws and guidelines.</p> <p>The Outbound Campaign Solution shall provide for multiple campaigns to be run simultaneously, (a minimum of ten).</p> <p>The Outbound Campaign Solution shall have the ability to create, amend, store, run and re-run a campaign.</p> <p>The Outbound Campaign Solution shall have the ability to continue a stopped or interrupted campaign where it left off on the list.</p> <p>The Outbound Campaign Solution shall provide an application that allows sites to build, manage, and monitor outbound campaign.</p> <p>The system shall allow call centers agents to place individual outbound calls when their responsibilities require them to do so. The system shall be able to track and report on outbound calls by agent, by team, and contact center.</p> <p>Reporting – Provide comprehensive historical, real time management, and exception reports.</p> <p>The CCS shall produce reports to document the results of the campaigns. These reports shall be easily configurable to reflect the nature of the campaign and prevent the same recipient from receiving repeated calls about the same matter.</p>	<p>Predictive dialing</p> <p>Ability to configure the number appearing on the called party caller ID for different campaigns</p> <p>Ability to run IVR only campaigns</p> <p>Ability to run live agent campaigns</p> <p>Ability to run Blended campaigns</p> <p>Ability to view a call's progress</p> <p>Ability to view a call's status</p> <p>Ability to generate reports on outbound campaign - call result (successful connection, no answer, duration )</p> <p>Ability to update VA data sources via industry standard interfaces, based on results from the outbound campaign</p> <p>Ability for customers to opt out of future outbound calls</p> <p>Ability to exclude parties that have opted out from outbound campaigns for future outbound campaigns</p> <p>Ability to review chat for quality assurance (QA)</p> <p>Ability to generate a QA sample of chats to be reviewed</p>
Text (SMS)		<p>Ability to configure routing texts based on the phone number associated with the text. Each short code or long number has its own routing plans.</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

		<p>Ability to review incoming or response texts, and identify key words for action. Such as STOP, PAYMENT, STATUS, RENEW, etc.</p> <p>Ability to provide a confirmation text to the user when a process is completed as requested</p>
Text Chat (Web Chat)	<p>The contractor shall provide contact center agents functionality to engage in real time, secure text chat with callers directed from its web site. The text chat shall provide the following minimum capabilities:</p> <p>The Chat system shall allow a user of one of VA's portals to request a secure chat session with an agent at VA, and shall be able to recognize to which call center and individual the request shall be directed based on the web site from where the request was originated.</p> <p>The Chat system shall be secure to allow transfer of PII and PHI. Chat sessions shall be encrypted with a minimum of 256bit SSL protocol, both for agents using the application and customers.</p> <p>The Chat system shall ensure that VA security protocols and policies such as 508 compliance, are not violated, trigger pop-up blockers, or invoke security alerts during a chat session. If the session initiator is authenticated, the Chat system shall be able to pass the session initiator's PII into the CRM system and automatically pop-up that customer's record for the agent.</p> <p>The Chat system shall be capable of integrating with CRM and KM solutions.</p> <p>For authenticated chats, all chat information captured shall be able to be integrated into the customer's record in CRM solution.</p> <p>Archive text chat sessions (create transcripts)</p> <p>Allow agents to manage multiple text chat sessions</p> <p>The Chat system shall allow agents to handle, if desired, multiple chat sessions simultaneously, and be allowed to copy and paste into chat session from other windows to share knowledge objects or links to web sites or documents and provide a built in spell checker.</p> <p>Allow file transfers</p> <p>View the active web page the text chat caller is on</p> <p>Provide a log of text chat sessions. The Chat system shall maintain a history of these sessions in</p>	<p>Ability to send SMS texts to individual customers and to groups of customers</p> <p>Ability to receive messages from customers</p> <p>Ability to receive messages sent to short published numbers</p> <p>Ability to classify texts</p> <p>Ability to configure business rules to classify inbound texts</p> <p>Ability to prioritize chat</p> <p>Ability to configure number of sessions per agent</p> <p>Ability to use pre-defined chat script Apply Chat Bots And collect info and Authenticate Chat users</p> <p>Ability to watch customer typing before sending chat.</p> <p>Ability to capture chat transcript Apply Chat Bots And collect info and Authenticate Chat users</p> <p>Ability to email chat transcript</p> <p>Click to call Want and Need</p> <p>Ability to categorize chat to inquiry/request type</p> <p>Embedded chat with agents / lead / supervisor</p> <p>Ability to incorporate chat based communication to customer's interaction history</p> <p>Ability to Escalate Chat</p> <p>Ability to take over Chat</p> <p>Ability to route chat request based on chat point of origin</p> <p>Ability to Route Chat</p> <p>Ability to assign request type and route to appropriate agent</p> <p>Ability to provide Canned responses and instructions</p>



# Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>accordance with National Archives and Retention Authority (NARA) and VA storage retention requirements.</p> <p>The Chat system shall allow the automated storage of each individual chat session. The Chat system shall store metadata with chat (e.g. date, time).</p> <p>The Chat transcript shall be stored in a repository within Chat System.</p> <p>Provide an automatic spell check and grammar check option that is enabled when typing in active session.</p> <p>Provide Supervisor tool for chat monitoring</p> <p>The Chat system shall allow supervisors to join a chat for support or to coach agents.</p> <p>The Chat system shall allow agents to transfer chats to other agents based on skill assignment used by this system.</p> <p>The Chat system shall store pre-defined responses to certain questions and the system to import them by click of a button or by copying and pasting.</p> <p>The Chat system shall connect the initiator of the session with an agent, and shall be capable of simultaneously populating a list of Knowledge Management (KM) resources for the agent based upon the session initiator input.</p> <p>The Chat system shall track agents who are designated to handle chat sessions and provide reporting on those interactions.</p> <p>The Chat system shall support Pre, Post and Offline surveys. The Chat system shall provide the ability to send automated question upon initiation.</p> <p>The Chat system shall provide the ability for session initiator to see that the agent is typing.</p> <p>The Chat system shall allow the agent to see if the session initiator is typing.</p> <p>Once the Chat Icon is clicked, the Chat system shall require the user to enter their "name". The Chat system shall allow the session initiator to enter information used to prioritize/route the chat.</p> <p>The Chat system shall provide the ability to display a customizable disclaimer which the user shall accept prior to chatting with an agent.</p> <p>The Chat system shall provide the ability to queue chats, with ability to display informational message (e.g., to provide Toll Free Number) when maximum number in queue is reached.</p> <p>The Chat system shall display a scenario based message to the customer when no chat is available (e.g. technical difficulties or outside of defined hours of operation).</p> <p>The Chat system shall be available on all internet</p>	<p>Ability to integrate with Knowledge Management</p> <p>Ability to access KM</p> <p>Ability transition from one communication channel to another</p> <p>Ability to Share/attach documents</p> <p>Ability to provide messages after hours</p> <p>Ability to provide intelligent routing based on chat content</p> <p>Ability to provide KM outside hours of operation</p> <p>Ability to capture Contact Information</p> <p>Ability to Authenticate customer via VA data sources, using standard industry interfaces</p> <p>Ability to retrieve Customer facts</p> <p>Ability to identify chat origination based on web page where chat is initiated</p> <p>Ability for Silent Monitoring</p> <p>Ability to view chat statistics</p> <p>Ability to view chat status</p> <p>Real Time Dashboard</p> <p>Ability to balance chat contact's work load</p> <p>Ability to review Chat</p> <p>Ability to integrate with Feedback tool</p> <p>Chat delivery reporting - number of requests, results, timing, origination, number of actual chat, # of chat drops</p> <p>Chat transcript attached to parent record</p> <p>Ability to search transcript using key words or expressions</p> <p>Need the ability to identify and link reply</p> <p>Need the ability to track response time out?</p> <p>Need the ability to resend failed texts for a specified number of</p>
--	---	---

# Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>browsers.</p> <p>The Chat system shall appear as a separate window on the screen with size configurable by the initiator.</p> <p>The Chat system shall allow an agent to join an in-progress chat.</p> <p>The Chat system shall provide a message to the session initiator and route to new agent if an agent becomes unresponsive.</p> <p>The Chat system shall allow agent to terminate session if user is unresponsive.</p> <p>An agent shall be able to join a chat in progress without interruption and have the ability to see the chat history</p> <p>If a chat gets transferred to another agent, the chat system shall move the transferred chat to a higher priority level.</p> <p>The Chat system shall allow either the user or agent to end the Chat session.</p> <p>Once a chat has been completed, the chat system shall allow agent to enter an outcome code, a call type and sub call type to complete chat session.</p> <p>The Chat system shall store and allow searches based on the following information:</p> <p>Name provided by user</p> <p>Self-check code provided by the user</p> <p>Chat Transcript</p> <p>Start and End date and time of Chat</p> <p>Call Type/Subtype</p> <p>Agent's name and station number.</p> <p>The Chat system shall allow supervisors to view agent's status and active chat sessions.</p> <p>The Chat system shall allow supervisors to view agent's production statistics (e.g., number of completed sessions since log-in, average chat duration, last log in, idle time since last chat completed, average time idle in shift).</p>	<p>times</p> <p>Need the ability for an Agent to view text messages</p> <p>Need the ability for an Agent to respond to text messages</p> <p>Need the ability to display to the external (non-VA) text recipient a custom text source number/identifier</p> <p>Need the ability to configure the number displayed as the send to the person being texted</p> <p>Need the ability to generate reports from text-based campaigns</p> <p>Need the ability to generate reports for inbound text contacts</p> <p>Need the ability to generate reports showing agents involved in text interactions</p> <p>Need the ability to generate reports based on text interactions and context such as length of transaction, average transaction, etc.</p> <p>Ability to generate sound and phone ringing once a new chat is initiated</p> <p>Request and process callbacks via chat</p> <p>Authenticated Chat and Non Authenticated , Anonymous Chats</p> <p>Ability to initiate from emailed link</p> <p>Ability to offer chat via pop up</p> <p>Chat statistics analytics</p>
--	---	--

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

		<p>Ability to initiate a chat session from a link (e.g., help button) on a website or page.</p> <p>Have the ability to screen capture a chat as part of the record</p>
Text Chat (Web Chat) – Additional Capabilities	The Chat system shall provide the customer's Internet Protocol (IP) number, if available.	
FAX Management		<p>Support virtual numbers</p> <p>Support agent-specific fax numbers</p> <p>Ability to send a fax from desktop</p> <p>Ability to convert documents received to PDF</p> <p>Ability to convert documents sent</p> <p>Centralized pull queue</p> <p>Centralized push queue</p> <p>Provide users ability to have a preset templates library</p> <p>Ability to select and use a template from the preset template library</p> <p>Ability to manage the templates within the preset templates library</p> <p>Integrate with an existing VA document repository system utilizing industry standard interfaces</p>
Web Call Back	The CCS shall provide the capability for a customer to request a call back by filling out a form or clicking a button on the agency's web site. The call back algorithm shall be based upon the availability of a contact center agent. The call back request shall be automatically distributed to the most appropriate agent based upon availability of an agent (within agency operating hours).	<p>Ability to request call back</p> <p>Ability to specify delay for call back (e.g. in five minutes)</p> <p>Ability to request call back for specific time (same day)</p> <p>Ability to request call back for specific time (different date)</p> <p>Ability to route call back requests based on web page where the request originated</p> <p>Ability to generate reports on call back calls as part of normal voice reporting</p> <p>Ability to report on number of call back requests generated</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

		using Web along with requestor Contact Information, call reason, call type, outcome
Web Call Through	<p>The CCS shall provide the capability to enable customers browsing the agency's web site the ability to call through (e.g. "click to talk") and simultaneously have a voice conversation with a contact center agent.</p> <p>Must meet Federal and VA security requirements.</p>	
Workforce Management	<p>The contractor shall provide a workforce management (WFM) system that automates forecasting and scheduling calculations based upon real time and historical contact center data. The WFM shall enable agencies to effectively schedule resources, accurately forecast call volumes and analyze/review performance statistics for single or multiple sites and blended applications. The workforce management system should provide the following minimum capabilities:</p> <p>Forecast staffing needs including agent skills, skill levels and shifts.</p> <p>Forecast contact volumes and workload - overall call volume and by contact channel.</p> <p>Forecasting functionality shall be used to predict future contact inbound and outbound traffic based on the historical data with breakdown by types and define necessary staffing to handle contacts within required service level.</p> <p>System shall be able to use historical contact center data directly or via regular import from telephony system for mid and short term forecasting and historical data from external sources for long-term forecasting and forecasting adjustments if necessary.</p> <p>System shall allow direct access to loaded historical data in view and edit modes. System shall allow marking of the historical data with abnormal events (first day after floating holiday) or any user – defined business related events (collection activities, new service offering, billing cycle) and use it in the forecasting models.</p> <p>System shall allow manual adjustments to forecasted data and keep sample version logs.</p> <p>System shall be capable of maintaining statistics with breakdown by call type, skill group or skill expression as defined in telephony system configuration.</p> <p>System shall be able to generate a forecast for entire</p>	<p>Historical data import - call / agent events - manual – Ability to pull historical data by Agency and LOB</p> <p>Historical data import - call / agent events - automatic batch</p> <p>Loaded historical data manual editing</p> <p>Abnormal days / events marking</p> <p>Ability to make manual forecast adjustment</p> <p>Synchronized with telephony system call type / skill view</p> <p>Consolidated forecast with site / call type breakdown</p> <p>Long term forecast (6-18) months - headcount planning</p> <p>Short term forecast (4 - 8 weeks) - day off planning</p> <p>Detailed forecast (daily / hourly breakdown) - daily schedules</p> <p>Support of "what - if" models with manual input</p> <p>13+ months "hiring and vacation" schedule</p> <p>3+ months "day off" schedule</p> <p>bi-weekly / weekly /daily staffing schedule</p> <p>Consolidated staffing requirements with location breakdown</p> <p>Ability to incorporate standing or ad - hock events</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>organization regardless of number of sites, skills and locations with following breakdown for each location and skill group. System shall be able to generate long-term forecast (6-18 month), short-term (month) and detailed (day, hourly, 30 and 15 minutes) intervals. System shall be able to produce under and over staffed staffing deviations from averages for each site or location under the same organization. System shall support modern modeling “what-if” scenarios and produce forecast for each sample of data in real time or near real time modes.</p> <p>Provide agent scheduling and create optimized agent schedules by shift and skill.</p> <p>Scheduling functionality allows to build and maintain actual staffing detailed work schedules based on forecasted data short term and define hiring needs long term.</p> <p>System shall be able to generate schedules for different periods – 13 months or more “vacation” schedule, 3 months “day off” schedule and monthly, bi-weekly and weekly detailed schedule.</p> <p>System shall be able to generate multiple versions / variations of the same schedule, show deviations from forecasted targets for each hourly or 30 minutes period, and allow selecting and publishing any version. Agent shall see only published version.</p> <p>Schedule generator must be able to take into consideration any standing events such as regular meetings, scheduled regular and ad hock training sessions for Agent, Agent or skill group, skill expression or team. System shall allow scheduling of both on the phone and off the phone activities according to work activities list as set in telephony system for not ready state and for complete off the phone activities in log off mode. System shall be able to generate different schedule templates with existing staff and criteria to determine the best possible shift types that will best support the forecasted volume during each 30 (or any other time unit) minute period.</p> <p>System shall be able to generate full-time and part-time schedules and use priorities set for each type of schedule. System shall allow agent and / or supervisor enter schedule / day / shift preferences and exercise priority system to resolve conflicting requests or bids for the same slots. System shall allow entering time off and vacation requests, allowed, used time tracking, and support approval workflow for supervisors and managers. Intra-day management is an effort to compensate unpredictable call volume and</p>	<p>Ability to enter vacation and time off request (sup / agent level)</p> <p>Ability to approve vacation and time off request (supervisor)</p> <p>Ability to see request status (agent)</p> <p>Ability to Bid for day of the week / shift</p> <p>Need the ability to analyze interaction trends across all channels and modalities</p> <p>Show consolidated adherence - enterprise groups or skills</p> <p>Shown over - under - staffing deviation per location</p> <p>Show forecasted call volume adherence</p> <p>Provide adherence from planned staffing</p> <p>Show adherence from key planned statistics</p>
--	--	---

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>staffing fluctuations. Intra-day management heavily relies on forecasting and scheduling tools specified above but in addition requires additional features to maintain desired performance. At minimum, intra-day management features shall include following:</p> <p>Real time reports or board displays showing queue and agent status. Ability to set up thresholds to receive immediate notification if threshold is exceeded (e.g. average wait time exceeds maximum allowed wait time)</p> <p>Ability to see forecasted staffing compared with current staffing (real time adherence), forecasted call volume compared to actual call volume. This information shall be available with breakdown by call type, skill group, skill expression or agent team</p> <p>Ability to re-assign agents to different skill groups / skills</p> <p>Ability to change call flow to direct calls to different group of agents or engage overflow to allow calls going to secondary group after primary group wait time exceeds threshold.</p> <p>Ability to maintain history of known factors affecting call volume and staffing and produce historical reports as necessary</p> <p>Ability to change agent/team schedule and distribute change notification real time or near real time.</p> <p>Ability to see in real-time and provide historical reports on agent adherence at the one minute level.</p>	
Virtual Queue	<p>The CCS shall provide a capability whereby callers can choose to remain waiting on-line for an attendant or receive a call back in turn.</p> <p>The Automatic Call Back Feature shall provide an Automatic Call Back scheduled by the system.</p> <p>The Automated Call Back feature shall present caller with option to hang up, but retain place in queue. The Automated Call Back feature shall configure the trigger point for virtual hold option based on:</p> <p>Queue depth (total number in queue)</p> <p>Time of day / week</p> <p>Average wait time</p> <p>Maximum wait time</p> <p>The Automated Call Back feature shall have the ability to query the caller on the call back to ensure re-connect is with original caller, to include options when it is not original caller that answers.</p> <p>Allow time for getting original caller</p> <p>Allow option to try again in 15 minutes (up to 2 times)</p>	<p>Need the ability to have virtual hold capability</p> <p>Need the ability to not impact the waiting time for those who opted to wait on hold or opted for a call back</p> <p>Need the ability for customer to schedule a call back rather than wait in a queue need the ability to schedule a call back during after hours</p> <p>Need the ability to generate reports on virtual hold statistics</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>The Automated Call Back feature shall capture current Calling Party Number (CPN), and allow user defined call back number.</p> <p>Must support DTMF entries, but speech recognition as secondary option is preferred as well.</p> <p>Allow entry of extensions.</p> <p>Restrict certain area codes (900, 977, etc.)</p> <p>The Automated Call Back feature shall configure re-dial attempts if call back is unanswered or receives fax.</p> <p>The Automated Call Back feature shall have the ability to leave recorded message if no answer on predefined number of attempts.</p> <p>Recorded message shall include personalized information, such as caller's name.</p> <p>The Automated Call Back feature shall limit the amount of virtual hold activity if desired</p> <p>The Automated Call Back feature shall have the ability to report virtual hold activity, including:</p> <ul style="list-style-type: none"><li>Failed call back attempts</li><li>Total calls utilizing virtual hold</li><li>Estimated wait time vs. wait time for actual first call attempt</li><li>Acceptance rate vs. stated queue depth</li></ul> <p>Schedule Call Back features:</p> <p>The Scheduled Call Back feature shall have the ability to provide callbacks scheduled by the callers' selection of time and date.</p> <p>The Scheduled Call Back feature shall have the ability to present caller with scheduled call back option based on configurable parameters.</p> <p>The Scheduled Call Back feature shall have the ability to configure the trigger point for scheduled call back option based on:</p> <ul style="list-style-type: none"><li>Queue depth</li><li>Time of day / week preferred by caller</li><li>Average wait time</li><li>Maximum wait time</li></ul> <p>The Scheduled Call Back feature shall have the ability to query the caller on the call back to ensure re-connect is with original caller.</p> <p>The Scheduled Call Back feature shall capture current CPN, and allow user defined call back number.</p> <p>Allow entry of extensions.</p> <p>Allow VA to build list of CPN's that can be blocked from call back in future – to prevent prank calls, or abuse of system.</p> <p>Restrict certain area codes (900, 977, etc.).</p>	
--	---	--

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>The Scheduled Call Back feature shall have the ability configure re-dial attempts if call back is unanswered.</p> <p>The Scheduled Call Back feature shall have the ability leave recorded message if no answer on predefined number of attempts.</p> <p>The Scheduled Call Back feature shall have the ability to limit the amount of scheduled call back activity if desired.</p> <p>The Scheduled Call Back feature shall have the ability to compare desired call back time and date to scheduled hours of operation.</p> <p>The Scheduled Call Back feature shall have the ability to limit number of scheduled callbacks within time buckets (15-minute segments).</p> <p>The Scheduled Call Back feature shall have the ability to prevent scheduled callbacks during projected busy times.</p> <p>The Scheduled Call Back feature shall have the ability to offer scheduled callbacks during closed hours.</p> <p>The Scheduled Call Back feature shall have the ability to offer a recommended time slot for callbacks.</p> <p>The Scheduled Call Back feature shall have the ability to report failed callbacks.</p> <p>The Scheduled Call Back feature shall have the ability to accommodate callers in multiple time zones.</p> <p>The Scheduled Call Back feature shall provide the ability to estimate time zone based on CPN (may be incorrect because of cell phones or other routing issues).</p> <p>The Scheduled Call Back feature shall provide the ability to identify and adjust time zone based on caller preference.</p>	
Automated Call Survey	<p>The Automated Call Survey shall connect to caller immediately following completion of a call automatically initiated by the IVR if caller has agreed to take survey.</p> <p>The Automated Call Survey shall allow responses based on touch-tone or voice inputs.</p> <p>The Automated Call Survey will allow for respondent comments (recordings) after each question and overall if desired. Recording be stored for at least 15 months.</p> <p>The Automated Call Survey shall allow call types to be assigned a delayed response survey.</p> <p>The Automated Call Survey shall allow a delayed response survey call back to be configured up to 5 days after the initial call was received.</p> <p>The Automated Call Survey shall maintain survey results for minimum of 15 months.</p> <p>Automated Survey management and reporting</p>	<p>Need the ability to conduct surveys callers</p> <p>Need the ability to survey Veterans post calls - outbound</p>



Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>The Automated Call Survey shall associate surveys to call types.</p> <p>The Automated Call Survey shall allow remote audio update to survey questions, and/or text to speech.</p> <p>9.The Automated Call Survey shall allow access permissions to be configurable.</p> <p>The Automated Call Survey shall allow surveys to be configured by VA staff with appropriate access permission.</p> <p>10.The Automated Call Survey shall provide web based or similar access to allow approved users to access information, regardless of VA location.</p> <p>11.The Automated Call Survey shall allow user to configure a scoring system of responses, to include weighting of responses in cumulative score.</p> <p>12.The Automated Call Survey shall allow the VA user to preview the surveys that have been configured:</p> <ul style="list-style-type: none"><li>Number of questions</li><li>Survey question content</li><li>Numerical survey choices (0-9)</li><li>Surveys associated with call types</li><li>Time delay prior to initiating a call back.</li></ul> <p>13.The Automated Call Survey shall include the following reporting requirements:</p> <p>14.The Automated Call Survey shall allow configuration of reporting results, down to a minimum of 30 minute segments, and up to a minimum of one year of results</p> <p>15.The Automated Call Survey shall record associated caller data (CPN), as well as original call data (e.g. date, time, Agent, IVR exit point) with the survey results of the caller.</p> <p>16.The Automated Call Survey shall allow for sorting, summing, and averaging of responses over custom time range.</p> <p>The Automated Call Survey shall allow for sorting, summing, and averaging of responses by organizational hierarchies from Agent level to Agency level.</p> <p>The Automated Call Survey shall allow for exporting of responses into CSV or similar format for use with Microsoft Suite products.</p> <p>The Automated Call Survey shall allow the exporting of data via industry standard interfaces (e.g., API, SQL) to external databases.</p> <p>17.The Automated Call Survey shall allow viewing, printing, and exporting to excel of all reports.</p> <p>18.The Automated Call Survey shall provide graphing and trending capabilities for each question using custom time ranges.</p>	
--	---	--

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	<p>19.The Automated Call Survey shall provide statistical functions such as average, mean, median, and standard deviation.</p> <p>20.The Automated Call Survey shall provide basic response count information, including non-response counts.</p> <p>21.The Automated Call Survey shall provide prompt survey results – preference for results within 1 hour of survey, but a maximum of 12 hours.</p> <p>22.The Automated Call Survey shall provide detail results of survey to the Agent and individual call level.</p> <p>23.The Automated Call Survey shall provide grouping of results to include summary by:</p> <ul style="list-style-type: none"><li>Teams</li><li>Contact center site</li><li>Business line</li><li>National levels</li></ul> <p>24.The Automated Call Survey shall provide review of results by survey question with results listed by day over user input range of dates.</p> <p>25.The Automated Call Survey shall track the following survey data:</p> <ul style="list-style-type: none"><li>Survey acceptance</li><li>Survey transmittal success rate</li><li>Survey completion rates</li></ul> <p>26.System shall provide access to respondent comments</p> <p>27.The Automated Call Survey shall provide the ability to allocate comments into categories as, compliment, general or compliant.</p> <p>28.The Automated Call Survey shall provide the ability for comments to be sorted by the following:</p> <ul style="list-style-type: none"><li>Date</li><li>Time</li><li>Type of comment</li></ul> <p>29.Customer Satisfaction (CSat) Survey</p> <p>Requirements are as follows (provided as a part of the Automated survey solution):</p> <p>The Automated Call Survey shall provide reporting metrics on CSat sessions to include total sessions, average session length, activity per Agent versus contact, and other common CSat metrics:</p> <p>The Automated Call Survey shall provide acceptance rates on CSat offers on web pages.</p> <p>30.The CSat service shall report the Time By 15 minute intervals.</p> <p>31.The CSat service shall report Sessions Offered (SO) – by 15-minute intervals.</p> <p>32.The CSat service shall report Average Handle Time (AHT) in MM: SS.TT.</p>	
--	--	--

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

	33.The CSat service shall report Percent Sessions Answered (PSA). 34.The CSat service shall report Service Object (SO) - the percent of time the targeted service objective was met. 35.The CSat service shall report Busies/failed contact. 36.The CSat service shall report Average Speed of Answer (ASA). 37.The Line of Business shall be identified on the Survey Report.	
Metrics Storage Requirements		Maintain a minimum of 2 years of history

## **5.10 OPTIONAL TASK FIVE – TRANSITION OUT**

### **5.10.1 TRANSITION-OUT TEAM AND REQUIREMENTS PLANNING**

If exercised, at the commencement of Transition-out service period, the Contractor shall appoint a suitable qualified representative as a single point of contact for the Transition-out services.

The Contractor shall identify and document all open items during the transition, determine a resolution date and obtain VA concurrence for any items that will not be closed prior to completion of the transition. The Contractor shall support the transition out period; provide on-site support to facilitate parallel transition and operations activities.

### **5.10.2 TRANSITION-OUT PLAN**

It is anticipated that some work requirements will be in progress through the phase-out period of this TO. The Contractor shall provide an orderly transition of work acceptance and accomplishment, so that impact to the managed CCS infrastructure services is minimal. Interruptions or delays to the work will not adversely impact the mission. Therefore, the Contractor shall provide for maximum cooperation with the successor while insuring that no services receive inadequate attention during phase-out. The Contractor shall plan for a 60-day transition period of work, to insure continuity of services during the phase-out period.

At the conclusion of this effort, the Contractor shall ensure a smooth transition during the next successor's phase-in period. The Contractor shall aid the next successor in the development of plans, procedures, and methods for assumption of all on-going work. The Contractor shall provide an orderly transition of work acceptance and accomplishment, so that full control by the successful offeror is achieved by the end of the phase-out period.

This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of all artifacts delivered under this

contract, as well as existing policies and procedures, and delivery of baseline metrics and statistics. The Contractor shall develop a Transition Plan for Government approval.

The Transition-Out Plan shall include, but is not limited to:

- The overall approach
- The key activities and operating results
- Any Acceptance criteria provided by and approved by the VA
- An outline of how the Contractor intends to work with VA or VA's designee(s) to ensure an orderly transfer of the services (the risks considered shall be clearly stated and an explanation shall be provided for how the Contractor's solution and approach will reduce the impact of these risks)
- Requirements for collaboration with VA or VA's designee(s) to ensure an orderly transition of the services
- Roles and responsibilities of the Contractor during the Transition-Out services period. The description of the Transition-Out for each function, including the methodology for the transfer of knowledge between the Contractor's personnel and the personnel who will be responsible for providing the services in the future
- Identification of risks in the transfer process, risk minimization strategies and preventive measures
- How the quality and level of the services and the Service Levels will be achieved during the Transition-Out Services period
- Considerations and work in the fields of security, disaster recovery and contingency planning during the Transition-Out Services Period
- Description from the Contractor as to how insufficiently documented Systems and Equipment are treated
- Description of Change and release management, including all approvals and certifications by VA
- As part of the Transition Out Plan, the Contractor shall submit a proposed diagram of how the transfer of the services will be organized
- The Contractor's description of the process for checking the Transition Out Plan, including the terms which state that VA may monitor such process
- Actions to support a smooth and uninterrupted transfer of all activities and services to a new vendor
- Transition of all historic data to new Contractor system.
- Transfer of hardware and software warranties (if any), maintenance agreements and licenses.
- Transfer of all necessary business and/or technical documentation.
- Transfer of all incoming contact channels including telephone numbers, email addresses, WebChat URLs, to the new Contractor or to the VA, as designated by VA.
- Turn-in of all Government keys, ID/access cards, and security codes.

Until the Transition-Out Plan is complete, the Contractor shall take appropriate action to update the Transition-Out Plan, including the impacts of issues and risks which are identified by the Contractor and VA. The Contractor shall also propose changes to the

Transition-Out Plan when asked to do so by VA at appropriate intervals. Changes to the Transition-Out Plan must be approved by VA in writing. The Contractor shall provide Weekly Transition Status Reports and maintain performance commitments during the Transition Period.

**Deliverables:**

- A. Transition-Out Plan
- B. Weekly Transition Status Reports

## **5.11 OPTION PERIOD**

If the Option Period(s) are exercised by VA, the Contractor shall continue to perform the tasks embodied in this PWS inclusive of all subparagraphs, and provide all requested deliverables for one (1) year. The Contractor shall continue to support all new functionality or Services incorporated by any exercised optional tasks.

## **6.0 GENERAL REQUIREMENTS**

### **6.1 ENTERPRISE AND IT FRAMEWORK**

#### **6.1.1 ONE-VA TECHNICAL REFERENCE MODEL**

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) located at <https://www.va.gov/trm/TRMHomePage.aspx>. 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.

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

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), [http://www.ea.oit.va.gov/VA\\_EA/VAEA\\_TechnicalArchitecture.asp](http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp), and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, [http://www.techstrategies.oit.va.gov/enterprise\\_dp.asp](http://www.techstrategies.oit.va.gov/enterprise_dp.asp). The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

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

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at:

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf>,

<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf>, and

<https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf> respectively. Contractor delivered applications and systems shall be on FIPS

201-2 the Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

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

1. Automated provisioning and are able to use enterprise provisioning service
2. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns, available at the techstrategies link above.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.

11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems.

<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846>

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

### **6.1.3 INTERNET PROTOCOL VERSION 6 (IPv6)**

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005

(<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf>) and September 28, 2010 (<https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf>). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (<https://www.nist.gov/programs-projects/usgv6-technical-basis-next-generation-internet>), the Technical Infrastructure for USGv6 Adoption (<http://www-x.antd.nist.gov/usgv6/index.html>), 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. In addition to the above requirements, all devices shall support native IPv6 and/or dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc.) shall support native IPv6 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure interoperability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: <https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282>.

### **6.1.4 TRUSTED INTERNET CONNECTION (TIC)**

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (<https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf>), M08-23 mandating Domain Name System Security (NSSEC) (<https://obamawhitehouse.archives.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 [https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC\\_Ref\\_Arch\\_v2-0\\_2013.pdf](https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf).

### **6.1.5 STANDARD COMPUTER CONFIGURATION**

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using 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 the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

### **6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)**

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at <https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371>. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products.

### **6.1.7 PROCESS ASSET LIBRARY (PAL)**

The Contractor shall utilize PAL, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.



## 6.2 SECURITY AND PRIVACY REQUIREMENTS

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

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

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

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

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5.10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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:

- 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.
- Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their

- background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 are to encrypt the file, use a secure fax, or use a traceable mail service.
- c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
  - d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    - 1) Optional Form 306
    - 2) Self-Certification of Continuous Service
    - 3) VA Form 0710
    - 4) Completed SIC Fingerprint Request Form
  - e. 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).
  - f. The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM is moving towards a "click to sign" process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via e-QIP).
  - g. 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.
  - h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC),

completed training delineated in VA Handbook 6500.6 (Appendix C, Section 9), signed “Contractor Rules of Behavior”, and with a valid, operational PIV credential for PIV-only logical access to VA’s network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled by OPM. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of OPM.

- i. 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.
- j. 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.
- k. 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 Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
-----------------------	----------------------	----------------------------------

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

A. Technical / Quality of Product or Service	<ol style="list-style-type: none"> <li>1. Demonstrates understanding of requirements</li> <li>2. Efficient and effective in meeting requirements</li> <li>3. Meets technical needs and mission requirements</li> <li>4. Provides quality services/products</li> </ol>	Satisfactory or higher (see Service Level Requirements in section 6.5.2)
B. Project Milestones and Schedule	<ol style="list-style-type: none"> <li>1. Established milestones and project dates are met</li> <li>2. Products completed, reviewed, delivered in accordance with the established schedule</li> <li>3. Notifies customer in advance of potential problems</li> </ol>	Satisfactory or higher
C. Cost & Staffing	<ol style="list-style-type: none"> <li>1. Currency of expertise and staffing levels appropriate</li> <li>2. Personnel possess necessary knowledge, skills and abilities to perform tasks</li> </ol>	Satisfactory or higher
D. Management	<ol style="list-style-type: none"> <li>1. Integration and coordination of all activities to execute effort</li> </ol>	Satisfactory or higher

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

## 6.5 SERVICE LEVELS

### 6.5.1 SERVICE LEVEL FRAMEWORK

This section sets forth the functional and technical specifications for the Critical Performance Indicators (CPI), and Key Performance Indicators (KPI) to be established between the Contractor and VA. This section contains the tables and descriptions that provide VA framework and expectations relating to service level commitments, and the implications of meeting versus failing to meet the requirements and objectives, as applicable. This section defines VA detailed performance, management, and reporting requirements for all Contractor Contact Center Service Delivery Services.

## Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

The method set out herein will be implemented to manage the Contractor's performance against each Service Level, in order to monitor the overall performance of the Contractor.

The Contractor shall be required to comply with the following performance management and reporting mechanisms for all Services within the scope of this PWS:

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

The performance metrics are directly related to the service level requirements set forth below. Please be advised that the Contractor is required to meet all requirements established by this PWS. However, if the Contractor's performance falls below a required service level, the Contractor shall only be paid for the lower level provided service level. Please be further advised that the VA's payment for the lower service level provided in no way waives the Government's right to pursue any remedies available by law, including, but not limited to, termination for breach of contract.

VA will begin assessing lower service level prices for all CPIs as described below, commencing with the third month of contract performance. The COR will notify the Contractor and CO in writing when any CPI metric has been missed. The first month a CPI metric is missed the Contractor will be assessed a two- percent (2%) lower price against the applicable CLIN(s) for that month. Each consecutive month a metric is missed the Contractor will be assessed a four-percent (4%) lower price against the applicable CLIN(s). If multiple metrics are missed, the Contractor will be assessed the applicable lower price for each metric missed. Example: If the Contractor misses CPIs for the Availability within Service Level metrics during the third month of performance then the Contractor shall be assessed a four-percent (4%) price reduction against the applicable CLIN(s)., as it has provided a lower then agreed to service level for 2 CPI metrics.

Prices for lower service levels will be assessed against the CPI metrics only as described in this section

If the contractor fails to meet any of the KPIs for Infrastructure SLAs and Operational SLAs for a given month, then the contractor must issue a credit. The credit is calculated as 12.5% of the Monthly Recurring Charge (MRC) for that service at that Agency Hierarchy Code. Further, if the contractor fails to meet the SLA performance objective for two consecutive months, the contractor must credit the Agency 25% of the MRC for that service; failure to meet the SLA performance objective for three consecutive months requires a credit of 50% of the MRC for that service. After the third consecutive month of failure to perform at the specified level, the Agency can discontinue the service without penalty, or can continue service inclusive of the 50% credit

## 6.5.2 SERVICE LEVEL REQUIREMENTS

The Contractor shall meet the Service Level Requirement for each Service Level set forth. The Service Level Requirements are provided in the following tables. The performance indicator type and associated requirement is specified. Refinement of the service level requirements will be part of the collaborative development of the Process and Procedures document.

### 6.5.2.1 INFRASTRUCTURE SERVICE LEVEL REQUIREMENTS (SLA)

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Availability (Service) ((Av(S))	Key	99.99%	No greater than 5 minutes of downtime per month	See Note 1
Voice Quality	Key	Mean Opinion Score (MOS) of 4.5	MOS $\geq$ 4.5	See Note 2

**Note 1: Availability (Service) ((Av(S))** – Availability is measured using the following formula:

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}}$$

Uptime is a fixed value of 43,200 calculated by normalizing the days in a month to 30 multiplied by the hours and minutes (30x24x60=43,200).

Downtime incidents and failures are defined as any condition which prevents the solution from providing services as designed in portion or its entirety at one or multiple answering sites. Downtime is the total minutes during which any of the services provided through the Components of Service listed below cannot be used by VA to perform their tasks.

**Uptime.** Managed Service Provider (MSP) will deliver 99.99% of Uptime per month for Components of Service, which are those specific Contact Center features required for contact delivery included in and used by VA. If MSP exceeds five (5) minutes (99.99% uptime) of Downtime in any given month, VA may request a disincentive for such Downtime associated with a trouble ticket (service request) submitted by an End User. Upon such request and MSP's verification of the trouble ticket and the Downtime, MSP will issue a disincentive to VA.

**Components of Service.** Contact Center components covered by this SLA include all mandatory features and all optional features procured as described in PWS.

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

**Note 2: Voice Quality** - MSP shall provide monthly report containing MOS scores using the following industry standard formula:

$$MOS = \frac{\sum_{n=0}^N R_n}{N}$$

### 6.5.2.2 OPERATIONAL SERVICE LEVEL REQUIREMENTS (SLA)

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Service Request – Agent Moves, Adds, Changes, Deletions (MACD)	Key	95% <i>(Established Performance Standard Thresholds are met 95% of the time or greater, no less than 90% of the time)</i>	Total time taken to complete the MACD request:  Addition/Modification/ Deletion of Agents / Users into all relevant systems will be done within 3 business days  Agent Skilling - add/change/delete or adjust priority of skills shall be done within 30 minutes from submission for daily resource staffing adjustments	Service Desk Request creation/completion timestamp, Measured Daily/Reported Monthly
Service Request – Queues or Skill Groups (MACD)	Key	95% <i>(Established Performance Standard Thresholds are met 95% of the time or greater, no less than 90% of the time)</i>	Total time taken to complete the MACD request:  Addition/Modification/ Deletion of Queues or Skill Groups of new queue or skill group, with ability to transfer or point IVR to the new queue, and provide reporting access on queue will be completed within 7 business days  Process a change in hours of operations for unplanned	Service Desk Request creation/completion timestamp Measured Daily/Reported Monthly

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
			closures due to weather or other events will be done within 30 minute of submission	
Service Request – IVR (MACD)	Critical	95% <i>(Established Performance Standard Thresholds are met 95% of the time or greater, no less than 90% of the time)</i>	Complete a prompt/Script change for emergency announcements on main menus within 30 minutes of submission.	Service Desk Request creation/completion timestamp Measured Daily/Reported Monthly
Service Request – IVR (MACD)	Critical	95% <i>(Established Performance Standard Thresholds are met 95% of the time or greater, no less than 90% of the time)</i>	For each new IVR request (to include complete new IVR menu flow, and associated skill groups, report creation, and testing), a project plan will be received within 5 business days.	Service Desk Request creation/completion timestamp Measured Monthly/Reported Quarterly
Help Desk Request – Non-MACD	Critical	95% <i>(Established Performance Standard Thresholds are met 95% of the time or greater, no less than 90% of the time)</i>	All requests responded to within 4 hours and resolved within 2 business days.	Service Desk Request creation/completion timestamp Measured Monthly/Reported Quarterly
IT Management / Agent- Customer Satisfaction Rating	Critical	80% (Quarterly)	The Service Level for IT Management - Customer Satisfaction Rating is the percentage of VA Agent/ IT Management survey responses for surveys undertaken	The total number of survey responses with an average rating of “satisfied” or better (within the Measurement Period) divided by the total number of survey responses completed and returned during the



Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
			in connection with CCS that are answered with an average rating of “satisfied” or better	Measurement Period, multiplied by one-hundred (100).
Event Notification (EN)  Service Impacting	Key	99% <i>(Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)</i>	Notification 30 days in advance of any Feature Changes  <i>(e.g., system refresh, patches/ Updates which will add, remove, change, or impact existing operator or user features or functions)</i>	Reports as provided through agreed upon Processes & Procedures (e.g., Enterprise Service Desk Request creation/completion timestamp)
	Key	99% <i>(Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)</i>	Notification 30 days prior to any event which may diminish service or system component availability  <i>(e.g., an event that impacts the Availability KPI)</i>	Reports as provided through agreed upon Processes & Procedures (e.g., Enterprise Service Desk Request creation/completion timestamp)
Event Notification (EN)  Security Breach <i>(as defined by NIST guidelines)</i>	Key	99% <i>(Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)</i>	Notification within 2 hours	Reports as provided through agreed upon Processes & Procedures (e.g., Enterprise Service Desk Request creation/completion timestamp)

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
<p>Response Time (RT)</p> <p>Service Availability Impacting</p>	Key	<p>99%</p> <p><i>(Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)</i></p>	<p>Provide immediate acknowledgement of any service impacting event (24 hours per day/7 days per week)</p> <p>Provide impact assessment and troubleshooting plan within 60 minutes of initial notification</p> <p>Provide status updates hourly through resolution.</p>	<p>Reports as provided through agreed upon Processes &amp; Procedures (e.g., Enterprise Service Desk Request creation/completion timestamp)</p>
<p>Training Compliance</p>	Key	<p>99%</p> <p><i>(Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)</i></p>	<p>Mandatory Training Compliance Percentage</p> <p>Training defined as part of Policy &amp; Process Manual (PPM) and dependent on employee role and responsibilities.</p>	<p>(Total number of compliant MSP employees) / (Total number of MSP Personnel) Measured Monthly/Reported Monthly</p>

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Business Continuity Plans Tested (MSP Locations)	Key	99% (Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)	Number of Business Continuity plans tested in the prior year	(Number of services with documented BCP test Results for prior year/Total number of business units/processes with documented BC Plans) Measured Annually/Reported Annually
Disaster Recovery Plans Tested (MSP Locations)	Key	100% (Established Performance Standard Thresholds are met 100% of the time, no less than 99.999% of the time)	Number of Disaster Recovery plans tested in the prior year	(Number of services with documented DR Test Results for prior year/Total number of services with documented DR Plans) Measured Annually/Reported Annually

Managed Contact Center Infrastructure Service

TAC Number: **TAC-18-XXXXX**

Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Disaster Recovery (DR) Documentation (MSP Locations)	Key	99% (Established Performance Standard Thresholds are met 99% of the time or greater, no less than 95% of the time)	Means the Service Provider's upkeep of DR records (DR plans) for DR systems. For any given record the lack of accuracy in any one attribute means the inventory record to be completely not accurate.	Number of audited records for the DR records of a sample for which the record is accurate / number of audited DR records *100 Measured Quarterly/Reported Quarterly

**Definition:**

MSP service shall include new services, moves, adds and changes completed by the MSP on or before the due dates. The Service and Change Request SLA shall be based on committed installation timeline intervals established in this SLA or due dates negotiated between Customer and Contractor documented on the Contractor's order confirmation notification.

## 6.6 KEY PERSONNEL

The key personnel specified in this contract are considered to be essential to work performance. At least 30 days prior to diverting any of the specified individuals to other programs or contracts (or as soon as possible, if an individual must be replaced, for example, as a result of leaving the employ of the Contractor), the Contractor shall notify the Contracting Officer and shall submit comprehensive justification for the diversion or replacement request (including proposed substitutions for key personnel) to permit evaluation by the Government of the impact on performance under this contract. The Contractor shall not divert or otherwise replace any key personnel without the written consent of the Contracting Officer. The Government may modify the contract to add or delete key personnel at the request of the contractor or Government.

## 6.7 FACILITY/RESOURCE PROVISIONS

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

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, 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 VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

**6.8 GOVERNMENT FURNISHED PROPERTY**

No Government Furnished Property will be provided as part of this effort.

DRAFT

## **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, CCS systems, 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 according to SLA table above. 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, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

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

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), 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](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](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**

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: <https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards> and <http://www.section508.gov/content/learn/standards>. A printed copy of the standards will



be supplied upon request. The Contractor shall comply with the technical standards as marked:

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

### **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. Acceptance and Acceptance Testing**

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

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

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

### **Deliverables:**

A. 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 CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
  - 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 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, 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](http://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 [https://www4.eere.energy.gov/femp/requirements/laws\\_and\\_requirements/energy\\_star\\_and\\_femp\\_designated\\_products\\_procurement\\_requirements](https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements). 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](http://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.

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**

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

### **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 Contractor/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 CO 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 1600.05, *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 CO 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 CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for



system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

#### **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 VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment*.

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 11 configured to operate on Windows 7 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, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

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 (c), 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, in accordance with the SLA's listed above.

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 in accordance with the SLA's listed above.

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 CO 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 in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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

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

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

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, PWS 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. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

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

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

- 1) Nature of the event (loss, theft, unauthorized access);
- 2) Description of the event, including:
  - a) date of occurrence;
  - b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
- 3) Number of individuals affected or potentially affected;
- 4) Names of individuals or groups affected or potentially affected;
- 5) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- 6) Amount of time the data has been out of VA control;
- 7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
- 8) Known misuses of data containing sensitive personal information, if any;
- 9) Assessment of the potential harm to the affected individuals;

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

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

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages 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-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

## **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) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior,



updated version located at  
<https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848>, relating to  
access to VA information and information systems;

- 2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;
  - 3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]
- b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.
- 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.