

**TRANSFORMATION TWENTY-ONE TOTAL TECHNOLOGY NEXT GENERATION (T4NG)**

**PERFORMANCE WORK STATEMENT (PWS)**

**DEPARTMENT OF VETERANS AFFAIRS**

Office of Information & Technology

Information Technology Operations and Services

Infrastructure Operations

**Transformation Support Services (TSS)**

**Date:** May 24, 2018

**TAC-**18-50649

**Task Order PWS Version Number:** 1.1

Contents

[1.0 BACKGROUND 5](#_Toc514938030)

[2.0 APPLICABLE DOCUMENTS 7](#_Toc514938031)

[3.0 SCOPE OF WORK 8](#_Toc514938032)

[3.1 APPLICABILITY 8](#_Toc514938033)

[3.2 ORDER TYPE 8](#_Toc514938034)

[4.0 PERFORMANCE DETAILS 9](#_Toc514938035)

[4.1 PERFORMANCE PERIOD 9](#_Toc514938036)

[4.2 PLACE OF PERFORMANCE 9](#_Toc514938037)

[4.3 TRAVEL OR SPECIAL REQUIREMENTS 10](#_Toc514938038)

[4.4 CONTRACT MANAGEMENT 10](#_Toc514938039)

[4.5 GOVERNMENT FURNISHED PROPERTY 10](#_Toc514938040)

[4.6 SECURITY AND PRIVACY 11](#_Toc514938041)

[4.6.1 POSITION/TASK RISK DESIGNATION LEVEL(S) 12](#_Toc514938042)

[5.0 SPECIFIC TASKS AND DELIVERABLES 13](#_Toc514938043)

[5.1 TASK ORDER PROJECT MANAGEMENT (FFP) 14](#_Toc514938044)

[5.1.1 SUPPORT MANAGEMENT 14](#_Toc514938045)

[5.1.2 CONTRACTOR PROJECT MANAGEMENT PLAN 15](#_Toc514938046)

[5.1.3 PROGRAM ONBOARDING 16](#_Toc514938047)

[5.1.4 PRIVACY TRAINING 17](#_Toc514938048)

[5.1.5 TECHNICAL KICKOFF MEETING 17](#_Toc514938049)

[5.1.6 PROGRAM MANAGEMENT REVIEW 17](#_Toc514938050)

[5.1.7 PROGRAM MANAGEMENT COMMUNICATION PLAN 17](#_Toc514938051)

[5.1.8 TECHNICAL PROFICIENCY 18](#_Toc514938052)

[5.2 REMEDIATION SUPPORT SERVICES (T&M) 19](#_Toc514938053)

[5.2.1 CRISP CONFIGURATION MANAGEMENT SUPPORT 19](#_Toc514938054)

[5.2.1.1 CONFIGURATION MANAGEMENT VULNERABILITIES SUPPORT 19](#_Toc514938055)

[5.2.1.2 ENTERPRISE VULNERABILITY REMEDIATION PLANNING 19](#_Toc514938056)

[5.2.1.3 PATCH AND VULNERABILITY SUPPORT 20](#_Toc514938057)

[5.2.1.4 BASELINE CONFIGURATION PROCESS SUPPORT 21](#_Toc514938058)

[5.2.1.5 CRISP FIELD OPERATIONS SUPPORT 22](#_Toc514938059)

[5.2.1.6 CRISP ONSITE SUPPORT 22](#_Toc514938060)

[5.2.1.7 TIER 1 AND 2 ONSITE SUPPORT 25](#_Toc514938061)

[5.2.1.8 TIER 3/4 ONSITE SUPPORT 26](#_Toc514938062)

[5.2.1.9 OPERATIONAL PROJECT SUPPORT 27](#_Toc514938063)

[5.2.1.10 CONFIGURATION SUPPORT 28](#_Toc514938064)

[5.2.1.11 ENTERPRISE SECURITY AND ANALYSIS SUPPORT 30](#_Toc514938065)

[5.2.1.12 INTEGRITY AND AVAILABILITY SUPPORT 31](#_Toc514938066)

[5.2.1.13 VULNERABILITY, DATABASE, AND OPEN VIRTUAL MEMORY SYSTEM (VMS) SCANNING AND ANALYSIS SUPPORT 34](#_Toc514938067)

[5.2.2 UNAUTHORIZED SOFTWARE SUPPORT 36](#_Toc514938068)

[5.2.2.1 SUPPORT FOR UNAUTHORIZED SOFTWARE 36](#_Toc514938069)

[5.2.2.2 UNAUTHORIZED SOFTWARE MANAGEMENT AND ANALYSIS 37](#_Toc514938070)

[5.2.3 SYSTEM DEVELOPMENT/CHANGE MANAGEMENT CONTROLS 38](#_Toc514938071)

[5.2.4 SYSTEM BACKUP CHANGE MANAGEMENT ANALYSIS 38](#_Toc514938072)

[5.2.5 ACCESS CONTROL SUPPORT 39](#_Toc514938073)

[5.2.6 TWO-FACTOR AUTHENTICATION IMPLEMENTATION SUPPORT 39](#_Toc514938074)

[5.2.7 INCIDENT RESPONSE AND METRICS SUPPORT 40](#_Toc514938075)

[5.2.7.1 INCIDENT RESPONSE PLAN AND SOP SUPPORT 40](#_Toc514938076)

[5.2.7.2 MASTER TICKET TRACKING AND METRIC SUPPORT 41](#_Toc514938077)

[5.2.7.3 CAT 3 TICKET TRACKING AND METRIC SUPPORT 41](#_Toc514938078)

[5.2.7.4 CHILD TICKET TRACKING AND METRIC SUPPORT 42](#_Toc514938079)

[5.2.8 SIEM-BASED LOG MONITORING IMPLEMNTATION SUPPORT 42](#_Toc514938080)

[5.3 IT OPERATIONS AND SERVICES (T&M) 44](#_Toc514938081)

[5.3.1 FISCAL AND FINANCIAL PLANNING SUPPORT 44](#_Toc514938082)

[5.3.2 IMPLEMENTATION MANAGEMENT SUPPORT 44](#_Toc514938083)

[5.3.3 PROJECT MANAGEMENT SUPPORT 45](#_Toc514938084)

[5.3.4 ADMINISTRATION AND CLERICAL SUPPORT 46](#_Toc514938085)

[5.3.5 TECHNICAL DOCUMENTATION SUPPORT 47](#_Toc514938086)

[5.3.6 BUSINESS PROCESS SUPPORT 48](#_Toc514938087)

[5.3.7 SHAREPOINT MANAGEMENT SUPPORT 49](#_Toc514938088)

[5.3.7.1 SHAREPOINT ADMINISTRATION SUPPORT 49](#_Toc514938089)

[5.3.7.2 CONTENT MANAGEMENT SUPPORT 49](#_Toc514938090)

[5.3.8 SECURITY ADMINISTRATION SUPPORT 50](#_Toc514938091)

[5.3.8.1 SECURITY ANALYSIS SUPPORT 50](#_Toc514938092)

[5.3.8.2 CLOUD SECURITY SUPPORT SERVICES 51](#_Toc514938093)

[5.3.8.3 INFRASTRUCTURE SECURITY SUPPORT 51](#_Toc514938094)

[5.3.8.4 CYBERSECURITY TRAINING 52](#_Toc514938095)

[5.3.9 APPLICATION MONITORING SUPPORT 52](#_Toc514938096)

[5.3.10 NETWORK AND INFRASTRUCTURE MONITORING SUPPORT 53](#_Toc514938097)

[5.3.11 SYSTEM ADMINISTRATION SUPPORT 54](#_Toc514938098)

[5.3.12 PLATFORMS AND STORAGE SUPPORT 56](#_Toc514938099)

[5.3.13 SYSTEMS QUALITY CONTROL SUPPORT 56](#_Toc514938100)

[5.3.14 DOMAIN INFRASTRUCTURE SUPPORT 57](#_Toc514938101)

[5.3.15 SYSTEMS ROUTINE MAINTENANCE SUPPORT 58](#_Toc514938102)

[5.3.16 CONFIGURATION MANAGEMENT (CM) SUPPORT 58](#_Toc514938103)

[5.3.17 CHANGE MANAGEMENT SUPPORT 60](#_Toc514938104)

[5.3.18 RELEASE MANAGEMENT SUPPORT 62](#_Toc514938105)

[5.3.19 ASSET MANAGEMENT AND LOGISTICAL SUPPORT 63](#_Toc514938106)

[5.3.20 DATABASE ADMINISTRATION SUPPORT 63](#_Toc514938107)

[5.3.21 SYSTEMS ARCHITECTURE SUPPORT 64](#_Toc514938108)

[5.3.22 ARCHITECTURE ASSESSMENT SUPPORT 65](#_Toc514938109)

[5.3.23 SYSTEMS ENGINEERING SUPPORT 65](#_Toc514938110)

[5.3.24 DESKTOP AND DEVICE ENGINEERING (DDE) SERVICES 66](#_Toc514938111)

[5.3.25 NETWORK AND TELECOMMUNICATION SUPPORT 67](#_Toc514938112)

[5.3.26 APPLICATION MANAGEMENT SERVICES 68](#_Toc514938113)

[5.3.27 APPLICATION ADMINISTRATION SUPPORT 71](#_Toc514938114)

[5.3.28 DESKTOP SUPPORT SERVICES 71](#_Toc514938115)

[5.3.29 DESKTOP PROVISIONING SUPPORT 73](#_Toc514938116)

[5.3.30 CONTINUITY OF OPERATIONS (COOP) SUPPORT 74](#_Toc514938117)

[5.4 TRANSITION PLAN (OPTIONAL TASK) 75](#_Toc514938118)

[6.0 GENERAL REQUIREMENTS 75](#_Toc514938119)

[6.1 PERFORMANCE METRICS 75](#_Toc514938120)

[6.2 SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS 76](#_Toc514938121)

[6.2.1 EQUIVALENT FACILITATION 77](#_Toc514938122)

[6.2.2 COMPATIBILITY WITH ASSISTIVE TECHNOLOGY 77](#_Toc514938123)

[6.2.3 ACCEPTANCE AND ACCEPTANCE TESTING 77](#_Toc514938124)

[6.3 SEGREGATION OF DUTIES 77](#_Toc514938125)

[6.4 ORGANIZATIONAL CONFLICT OF INTEREST 78](#_Toc514938126)

[APPENDIX A 79](#_Toc514938127)

# BACKGROUND

The Office of Information & Technology (OIT) serves the Department of Veterans Affairs (VA) as a Veteran-centric provider of secure and cost-effective technology services. OIT collaborates with its business partners to create the best experience for all Veterans by endeavoring to provide a seamless and unified Veteran experience via state-of-the-art information technology (IT) solutions and service delivery. Within OIT, Information Technology Operations and Services (ITOPS) provides enterprise-level infrastructure engineering, system implementation, production operations, and IT service management. ITOPS is responsible for the design, testing, deployment, and sustainment of platforms and supporting infrastructure. ITOPS is OIT’s largest directorate with more than 6,000 IT professionals across the United States and its territories.

The largest component of ITOPS is Service Operations (SO), which has full accountability and responsibility for all system operations and production service delivery across the agency. SO is comprised of four major divisions: End User Operations (EUO), Infrastructure Operations (IO), Enterprise Command Operations (ECO), Enterprise Security Operations (ESO), and the new Service Management Office (SMO).

EUO provides onsite and remote support to IT customers across all VA Administrations and special program offices, including direct support of over 340,000 VA employees and thousands of contractors who are issued government-furnished IT equipment and accesses. EUO provisions computing devices, conducts new facility activations and performs move, adds and changes; executes local systems implementations; performs break/fix functions; and engages with VA’s customers across the nation to meet IT support needs. EUO is comprised of over 3,000 VA staff providing support at over 1,400 VA facilities in addition to supporting remote IT users.

IO has responsibility for management and 24x7x365 operation of the agency’s IT infrastructure, enterprise IT systems and data centers, which handle the data processing of Veterans’ health information and nearly $100 billion in Veterans’ benefits, payments and payroll processing for the Department. IO manages and operates IT infrastructure and systems supporting all agency Administrations and functions, including the Veterans Health Administration, Veterans Benefits Administration, and National Cemetery Administration, as well as VA’s special program offices. This organization provides operations, change control, security and Tier 3 support for enterprise systems, platforms, operating systems, storage, backups, file system management, back office, database, client technologies and mainframe; and enterprise call center infrastructure; as well as website and enterprise-based application hosting services. IO provides data processing services not only to VA but to other Federal agencies. The IO organization is comprised of over 2,000 government employees.

ECO includes the Enterprise Command Center and Enterprise Service Desk. The Enterprise Command Center provides proactive monitoring of systems to ensure compliance with service level agreements; reactive response to incidents achieving service restoration; and remediation efforts to report on and mitigate repeat incidents. The Enterprise Service Desk serves as the initial single point of contact for all VA IT customers for requesting IT services or reporting IT incidents. Enterprise Service Desk provides Tier 1 support 24x7x365, including end-to-end ticket management, and manages the restoration process for service outages. Enterprise Service Desk also manages notifications and After Action Reporting on service disruptions.

ESO ensures the privacy, confidentiality, integrity, and availability of VA information assets, and advises on information security initiatives as a trusted principal advisor. ESO includes Security Customer Support and Security Systems Support. The Security Customer Support team is dedicated to district and area level support, which provides “boots on the ground” for all VA facilities for local audit support, incident response , research and contracting support, and local risk management activities in addition to security awareness training. The Security Systems Support section is dedicated to enterprise-level maintenance providing common security services to customers and is responsible for infrastructure and applications security support including data center support, research support, Cybersecurity Risk Management Framework, specialized device support, business requirements support and field program support.

The new SMO provides oversight and governance of OIT’s IT Service Management (ITSM) tool and the IT Infrastructure Library (ITIL) processes that are the foundation of OIT’s service delivery framework. Processes and supporting ITSM tool modules overseen by this office include Service Catalog, Request Management, Service Desk, Incident Management, Problem Management, Change Management, Configuration Management, Release Management, and more.

Solution Delivery (SD) is the engineering arm of ITOPS. SD is responsible for engineering solutions that meet the needs of the Veteran and support the internal business requirements of VA. SD consists of four divisions: Business Systems Engineering, Infrastructure Engineering, Endpoint Engineering, and Security Engineering. The specialized engineering disciplines supported are Health Systems, Interagency Systems, Storage, Network, Platform, Data Center, Security, Video, Cloud, Messaging, Authentication, Personal Computers, Laptops, and Mobile Devices.

Service Management and Planning enables ITOPS to increase effectiveness and efficiency through central services supporting ITOPS. These enabling services include capital investment planning and management; multi-year programming, budget formulation and management; Contracting Officer Representative (COR) services for national IT infrastructure and operations contracts; executive correspondence and external reporting; strategic communications, ITOPS-wide action management; workforce and personnel administration services; ITOPS resource request management; central IT implementation management services; and oversight of the Enterprise Infrastructure Solutions program for telecommunications contracts.

Business Systems Engineering provides solutions for VA business service requirements supported by Infrastructure and End-Point Engineering. This engineering team collaborates with VA business entities, Government agencies, and private health organizations to ensure enterprise alignment with VA strategic goals and objectives. Infrastructure Engineering Engineers build standards-based enterprise infrastructure including networks, platform, storage, data center, and database services. These services include Wide Area Network (WAN)/Local Area Network (LAN) Infrastructure/Provisioning, Data Center Engineering and the Telecom Provisioning Office. Endpoint Engineering is responsible for creating and maintaining all baselines related to endpoint technologies. This engineering team is responsible for technology life-cycle changes for all endpoints, Messaging and Authentication Engineering, Business Voice/Call Center/Video Engineering, Enterprise Endpoint Management and Reporting, Mobile Technology, Endpoint Security Engineering, and Desktop and Device Engineering. Security Engineering provides the Department with an analytical security engineering foundation that delineates the principles and functions to meet the Department’s requirements, such as business needs and to reinforce compliance with VA Policy and other associated Federal mandates. This team engineers standards-based, policy-compliant security for the network enterprise and endpoint capabilities.

# APPLICABLE DOCUMENTS

The Contractor shall comply with the following documents, in addition to the documents in Section 2.0 in the T4NG Basic Performance Work Statement (PWS), in the performance of this effort:

1. Software Engineering Institute, Software Acquisition Capability Maturity Modeling (SA CMM) Level 2 procedures and processes
2. NBS SP500-153, “Guide to Auditing for Controls and Security: A System Development Life-Cycle Approach,” April 1988
3. Defense Information Systems Agency (DISA) Application Security and Development Security Technical Implementation Guide (STIG)
4. Electronic Signatures in Global and National Commerce Act
5. Federal Information Security Control Audit Manual (FISCAM)
6. IEEE (ISO/IEC) 12207, Standard for Information Technology Software Life Cycle Processes (in May 1998, replaced MIL-STD 498, Software Development and Documentation; which in November 1994, replaced DOD-STD-2167A, Defense System Software Development)
7. VA, Office of the Inspector General, Federal Information Security Management Act Audit for Fiscal Year 2013 (13-01391-72), May 29, 2014

The Contractor shall comply with the most recent version of any of the documents listed above. Additionally, the Contractor shall comply with any newly issued rules, regulations, instructions, handbooks, memoranda, or other Federal documents relating to security and privacy.

# SCOPE OF WORK

The Contractor shall provide IT enterprise support services to ITOPS in order to sustain ITOPS operations and remediation support services. ITOPS is evolving based on the ChooseVA reorganization and ITOPS support services will be evolving throughout the Task Order (TO) where performance and support may be adjusted in order to support consolidating, transforming, and modernizing IT services across the enterprise.

## **APPLICABILITY**

This TO effort PWS is within the scope of Section(s):

4.1 Program Management, Strategy, Enterprise Architecture and Planning Support

4.1.1 Strategy and Planning

4.1.2 Standards, Policy, Procedure and Process Development, and Implementation Support

4.1.3 Requirements Development and Analysis Support

4.1.5 Studies and Analyses

4.1.8 IT Services Management Support

4.2.3 IT Service Management Implementation

4.2.4 Enterprise Application/Services

4.2.5 Cloud Computing

4.2.9 System/Software Integration

4.2.12 Engineering and Technical Documentation

4.2.13 Current System and Data Migration

4.4 Test & Evaluation (T&E)

4.6 Enterprise Network

4.7 Enterprise Management Framework

4.8 Operations and Maintenance (O&M)

4.9 Cyber Security

4.11 Information Technology Facilities

## ORDER TYPE

The effort shall be proposed on a hybrid Firm-Fixed-Price (FFP) and Time-and-Materials (T&M) basis, including travel.

Tasks set forth under PWS Section 5.1 and all its subsections shall be performed on a FFP basis. Tasks set forth under PWS Sections 5.2 and 5.3, including all subsections shall be performed on a T&M basis. All travel shall be on a cost reimbursable, no fee basis. All tasks 5.1 through 5.3 shall be performed in the base and option periods, if exercised.

Overtime will not be approved under this order. It will not be approved for individual Contractor personnel exceeding his/her tour of duty.

# PERFORMANCE DETAILS

## PERFORMANCE PERIOD

The period of performance (PoP) shall be 12 months from date of award, with two 12-month option periods, if exercised by the Government.

## PLACE OF PERFORMANCE

Efforts under this TO shall be performed at Contractor facilities (offsite) and at Government facilities (onsite). The required onsite support is identified in Sections 5.1 through 5.3, if applicable. If onsite is not identified, then offsite support is anticipated.

The Contractor shall provide support to any of the VA facilities listed in Attachment 001 which is subject to change throughout the life of the TO PoP.

***Figure 1. VA Districts***

At VA facilities identified in Attachment 001, standard hours of operation, for a normal work day, is Monday through Friday (onsite and offsite) for eight hours within the hours from 6:00 AM to 10:00 PM, locations local time, and coordinated with the Government official at that site. Flexible work hours, such as staggered shifts, shall be required to meet the standard hours required above by facility.

In addition, Contractor performance may require the utilization of resources during non-standard hours of operation, including 24/7 operations, to respond to established scheduled maintenance activities that cannot be performed during standard hours since minimal interruption of service to VA staff or systems is required. The Contractor shall be required to adjust resource support accordingly as overtime will not be reimbursed under scheduled maintenance occurrences.

The Contractor may be required to support emergency changes, which are outside the scheduled maintenance occurrences, and will not be reimbursed on an overtime basis.

## TRAVEL OR SPECIAL REQUIREMENTS

The Government anticipates travel under this effort throughout the period of performance. All travel will be on a cost reimbursable, no fee basis. Travel and per diem shall be in accordance with the Federal Travel Regulations (FTR) and requires advanced concurrence by the Contracting Officer’s Representative (COR). Each Contractor invoice shall include copies of all receipts that support the travel costs claimed in the invoice. The Government will not reimburse local travel, which is travel within a 50-mile radius of an assigned duty location.

Requests for travel approval shall:

1. Be prepared in a legible manner
2. Be summarized by traveler
3. Identify the contract line item number (CLIN) and PWS task associated with the travel

## CONTRACT MANAGEMENT

All requirements of Sections 7.0 and 8.0 of the T4NG Basic PWS apply to this effort. This TO shall be addressed in the Contractor’s Progress, Status and Management Report as set forth in the T4NG Basic contract. The Contractor shall ensure the report is tailored to include dividing it into individual subsections based on the lowest level individual subtasks listed in sections 5.2 and 5.3 of this PWS.

## GOVERNMENT FURNISHED PROPERTY

The Government has determined that remote access solutions involving Citrix Access Gateway (CAG) have proven to be an unsatisfactory access method to complete the tasks on this specific TO. The Government also understands that GFE is limited to Contractors requiring direct access to the network to perform required tasks.

Based on the Government assessment of remote access solutions and the requirements of this TO, the Government estimates that the following GFE will be required by this TO:

1. 850 of standard laptops

2. 200 of developer-grade laptops

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

The Contractor shall be provided access to all available Government furnished information, facilities, material, equipment, or services as required to accomplish the efforts in the PWS for all onsite support. This shall include Cubicle, desk, telephone, chair, computer, shared printer, cell phones for callback and requisite consumable materials (i.e. office supplies).

The Contractor may be provided keys or codes for access to the Government facility, and if so, the Contractor shall control, track, and protect these keys and codes. Upon completion of the PoP, all keys and/or access badges to the Government facility shall be turned in to the COR.

The Contractor may have access to ITOPS IO currently installed version Microsoft Word, Excel, Visio, PowerPoint, and SharePoint as available, for VA provided devices.

## SECURITY AND PRIVACY

All requirements in Section 6.0 of the T4NG Basic PWS apply to this effort. Specific TO requirements relating to Addendum B, Section B4.0 paragraphs j and k supersede the corresponding T4NG Basic PWS paragraphs, and are as follows,

1. 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, but in no event longer than 3 days.
2. 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 within 3 days.

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 Request for Task Execution Plan (RTEP) and shall comply with VA Directive 6066.

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

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

Position Sensitivity and Background Investigation Requirements by Task

|  |  |  |  |
| --- | --- | --- | --- |
| **Task Number** | **Tier 1 (NACI)** | **Tier 2S (Standard MBI)** | **Tier 4S(Standard BI)** |
| 5.1 |  |  |  |
| 5.1.1 | [ ]  | [x]  | [ ]  |
| 5.1.2 | [ ]  | [x]  | [ ]  |
| 5.1.3 | [ ]  | [x]  | [ ]  |
| 5.1.4 | [ ]  | [x]  | [ ]  |
| 5.1.5 | [ ]  | [x]  | [ ]  |
| 5.1.6 | [ ]  | [x]  | [ ]  |
| 5.2 |  |  |  |
| 5.2.1 | [ ]  | [x]  | [ ]  |
| 5.2.2 | [ ]  | [x]  | [ ]  |
| 5.2.3 | [ ]  | [ ]  | [x]  |
| 5.2.4 | [ ]  | [ ]  | [x]  |
| 5.2.5 | [ ]  | [ ]  | [x]  |
| 5.2.6 | [ ]  | [ ]  | [x]  |
| 5.2.7 | [ ]  | [x]  | [ ]  |
| 5.2.8 | [ ]  | [ ]  | [x]  |
| 5.3 |  |  |  |
| 5.3.1 | [ ]  | [x]  | [ ]  |
| 5.3.2 | [ ]  | [x]  | [ ]  |
| 5.3.3 | [ ]  | [x]  | [ ]  |
| 5.3.4 | [ ]  | [x]  | [ ]  |
| 5.3.5 | [ ]  | [x]  | [ ]  |
| 5.3.6 | [ ]  | [x]  | [ ]  |
| 5.3.7 | [ ]  | [x]  | [ ]  |
| 5.3.8 | [ ]  | [ ]  | [x]  |
| 5.3.9 | [ ]  | [ ]  | [x]  |
| 5.3.10 | [ ]  | [ ]  | [x]  |
| 5.3.11 | [ ]  | [ ]  | [x]  |
| 5.3.12 | [ ]  | [ ]  | [x]  |
| 5.3.13 | [ ]  | [ ]  | [x]  |
| 5.3.14 | [ ]  | [ ]  | [x]  |
| 5.3.15 | [ ]  | [x]  | [ ]  |
| 5.3.16 | [ ]  | [x]  | [ ]  |
| 5.3.17 | [ ]  | [x]  | [ ]  |
| 5.3.18 | [ ]  | [x]  | [ ]  |
| 5.3.19 | [ ]  | [ ]  | [x]  |
| 5.3.20 | [ ]  | [ ]  | [x]  |
| 5.3.21 | [ ]  | [ ]  | [x]  |
| 5.3.22 | [ ]  | [ ]  | [x]  |
| 5.3.23 | [ ]  | [x]  | [ ]  |
| 5.3.24 | [ ]  | [x]  | [ ]  |
| 5.3.25 | [ ]  | [x]  | [ ]  |
| 5.3.26 | [ ]  | [ ]  | [x]  |
| 5.3.27 | [ ]  | [ ]  | [x]  |
| 5.3.28 | [ ]  | [x]  | [ ]  |
| 5.3.29 | [ ]  | [x]  | [ ]  |
| 5.3.30 | [ ]  | [ ]  | [x]  |

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.

The Government will support coordinating physical access to qualified and cleared personnel to the regional premises and facilities and to other Government sites (may include joint Department of Defense [DOD]/VA facilities).

A Tier 4S (Standard BI) is currently needed, for all Security, Network, and IT Administration positions requiring access to critical systems and for other positions as identified by the COR on an “as required” basis.

Personnel supporting the Network Security Operations Center (NSOC), the Medical Device Program, cybersecurity requirements may require a Secret Security Clearance and specialized security certifications. The Contractor may be required to have a valid active Secret Security clearance upon the start of performance of any of these tasks as applicable and shall remain active throughout the PoP of the task(s).

# SPECIFIC TASKS AND DELIVERABLES

The Contractor shall coordinate with the COR/VA Program Manager (PM) to review the Contractor’s Project Management Plan and its contents in accordance with Section 5.1.1 below for completing each deliverable and performing each task, prior to commencement of the task.

The Contractor shall perform the following:

## TASK ORDER PROJECT MANAGEMENT (FFP)

### Support Management

The Contractor shall provide a Project Manager (PjM) who shall serve as the manager of the TO and shall be the Contractor’s single point of contact for VA CORs and ITOPS management. The PjM shall manage the tasks, schedules, and analyze work discrepancies, communicate policies, purposes, and goals of the organization to the Contractor personnel for all projects. The PjM shall analyze and resolve programmatic issues, facilitate information exchange, and enhance management coordination as coordinated with the TO COR/VA PM(s). This support shall include managing onsite and offsite Contractor support, any tracking of resources across projects, transitioning and onboarding of new Contractor support required, and scheduling to ensure Support Services for ITOPS supported organizations for resolution of issues.

The Contractor PjM shall:

1. Conduct weekly VA Project Progress Reviews (PPR).

2. Provide Monthly Management Reports.

3. Track deliverables across projects.

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

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

6. Track Contractor support across projects on a daily basis.

7. Maintain a VA provided document management system e.g. SharePoint, to track project deliverables.

8. Track that all Contractor support:

1. Meets all task schedules including non-standard work schedule(s) as required. Schedules include; nights, weekends, and holidays in accordance with ITOPS requirements a nonstandard work schedule, if required. Work may be required beyond normal duty hours, including nights, weekends, and holidays as necessary.
2. Performance is tracked against the PWS requirements and performance metrics.

9. Provide a Program Management Office (PMO) to support the PM functions for managing the program across all sites, functions and major initiatives. The Contractor (e.g. PMO) shall:

1. Ensure compliance with all contract and government regulations (i.e. Section 2).
2. Monitor performance/compliance.
3. Respond to customer data calls.

### Contractor Project Management Plan

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

The purpose of the CPMP is to provide a tool to allow VA to effectively manage this T&M task order as well as report/reprioritize activities on a monthly basis. The CPMP shall address program integration and communication activities to include disseminating communications, developing documents, plans and briefs, and managing program interdependencies.

The CPMP shall contain the following:

1. Risk and Issue Register- identify risks and define and manage mitigation strategies.
2. Master Schedule-the Master Schedule shall incorporate the individual organization’s program/project milestones and schedules. The Master Schedule shall present each individual organization milestones and schedules for task completion.
3. Work Breakdown Structure (WBS), activity lists and resources, plan and work schedule (including dependencies and interdependencies), and a project baseline.

The CPMP data elements required by each organization and its activities include:

1. Project and specific activities.
2. Overview and description of the activity.
3. Overall high level assessment of progress of the activity
4. All work in-progress and completed for the activity during the week.
5. Identification of any contract related issues/risks uncovered during the previous week, especially highlighting those areas that have a high probability of impacting schedule, cost, or performance goals and their likely impacts on schedule, cost, or performance goals.
6. Explanations for any unresolved issues/risks, including possible solutions and any actions required of the Government and/or Contractor to resolve or mitigate any identified issue, including a plan and timeframe for resolution.
7. Status of previously identified issues/risks, actions taken to mitigate the situation, and/or progress made in rectifying the situation.
8. Work planned for the subsequent week.
9. Current activity schedule overlaid on original activity schedule showing any delays or advancement in schedule.
10. Current expenditures overlaid over the original budget showing any deviations in the actual expenditures versus the original budget and versus the current budget.
11. Workforce staffing data showing all Contractor personnel performing on the effort during the previous week. After the initial labor baseline is provided, each Weekly Work Plan Report shall identify any changes in staffing identifying each person who was added to the activity or removed from the contract. This should also include any planned travel for the activity.
12. Original schedule of deliverables and the corresponding deliverables made during the previous week.

The Contractor shall continuously monitor performance and report any deviation from the CPMP to the COR and VA PM during routine, regular communications. The Contractor shall respond to all COR queries related to project milestones and schedule within four business hours of receipt of written request.

**Deliverable:**

1. Contractor Project Management Plan

### Program Onboarding

The Contractor shall manage the onboarding of its staff. Onboarding includes steps to obtain a VA PIV card, network and email account, complete training, initiate background investigations, and gain physical and logical access.

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

**Deliverable:**

1. Weekly Onboarding Status Report

### Privacy Training

The Contractor shall submit status of VA Privacy and Information Security Awareness training for all individuals engaged on the TO. The status reporting shall identify the following information: a single Contractor Security Point of Contact (POC), the names of all personnel engaged on the task, their initial training dates for VA Privacy and Information Security training, and their next required training dates. This information shall be submitted as part of the Weekly Onboarding Status Report.

### Technical Kickoff Meeting

The Contractor shall hold a technical kickoff meeting within 10 days after TO award. The Contractor shall present, for review and approval by the Government, the details of the intended approach, work plan, and project schedule for each effort. The Contractor shall specify dates, locations (can be virtual), agenda (shall be provided to all attendees at least five (5) 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 Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM, and the designated Contractor Task Managers for each task. The Contractor may be required to conduct additional Kickoff meetings at the discretion of the COR for awarded option periods and optional tasks depending on the complexity of the options exercised.

### Program Management Review

The Contractor shall conduct monthly Program Management Reviews (PMRs) detailing the previous period’s achievements and progress on emerging and existing activities, identified risk and recommendations to mitigate risk, staffing plans and forecasts, as well as a financial analysis of contract expenditures. The COR may adjust the frequency of these meetings during performance. The Contractor shall deliver PMR briefing slides to the COR two (2) days prior to the scheduled monthly PMR. The Contractor shall document the PMR in minutes that shall include a list of action items.

As determined by the COR/VA PM, the PMR shall be conducted in person or virtually, by video or telephone conferencing or by Lync, the VA National Teleconferencing System (VANTS), or other conferencing capabilities within VA and Contractor capabilities.

### Program Management Communication Plan

The Contractor shall develop a single VA Enterprise Communication strategy which reaches across the ITOPS components supported in the PWS and shall be delivered to the COR/VA PM within 90 days of task award. The VA Enterprise Communication strategy shall be tailored to each of the ITOPS components to disseminate vulnerabilities to all VA organizations (e.g., Individual facilities). The Contractor shall maintain, update, and execute the strategy every 90 days thereafter for the life of the TO once reviewed, approved and implemented.

**Deliverable:**

1. VA Enterprise Communication Strategy

### TECHNICAL PROFICIENCY

The Contractor shall provide personnel that are fully trained in their assigned technical field of expertise and maintain technical proficiency and currency during the TO period of performance. If the Contractor requires training, the acquisition of this training shall be the Contractor’s responsibility, unless the training is Government required and provided at no cost to the Government via Training Management System (TMS).

All personnel performing work shall possess experience in the disciplines and technical areas described in each task which are related to the design, analysis, engineering, operation, maintenance, and security of the Data Centers.

It is the responsibility of the Contractor to provide Contractor support personnel and subcontractors who have the required educational background, experience, VA or DoD security clearance, and access authorization or combination thereof to meet the labor category descriptions under this TO for the T&M tasks.

Certain skilled experience professional and/or technical personnel are essential for accomplishing the work to be performed. The labor categories identified below are considered to be key to supporting this effort and shall not be removed from the TO effort, replaced or added to the TO without a compelling reason and without written notification to the COR and Contracting Officer (CO). If any change to the labor categories identified below becomes necessary (substitutions or additions), the Contractor shall immediately notify the COR and/or CO in writing, accompanied by the resume, if applicable, of the proposed replacement personnel who shall be of at least substantially equal ability and qualifications as the individuals currently performing in that category. It is expected that substitution or replacement of all the personnel outlined below will not occur within the first 90 days after date of TO award. Such labor categories and specific roles and responsibilities are further defined Section below:

1. Project Manager
2. Program Manager
3. Systems Administrator
4. Systems Administrator, Senior
5. Application Administrator
6. Database Administrator, Senior
7. Cyber Security Specialist, Senior
8. Software/Systems Architect, Sr.
9. System Security Engineer
10. Security Analyst, Senior\
11. Security Technician
12. Disaster Recovery Manager

The Contractor shall provide technical proficiency and expertise for the critical labor categories listed above as described in the related sections of the PWS.

## REMEDIATION SUPPORT SERVICES (T&M)

### CRISP CONFIGURATION MANAGEMENT SUPPORT

The Contractor shall support the configuration management controls and security protection tasks described below. This support is required across all components of ITOPS to support the implementation of all recommendations identified in this PWS and future Federal Information Security Management Act (FISMA) and Federal Information System Controls Audit Manual (FISCAM) audit recommendations. The configuration management support may be adjusted to reflect any changes resulting from the pending ChooseVA reorganization.

The Contractor shall provide support services to ITOPS and field facilities for resolving any critical material weaknesses (MW) as well as findings and recommendations related to configuration management, as identified by the VA Office of Inspector General (OIG) FISMA and FISCAM audits.

#### CONFIGURATION MANAGEMENT VULNERABILITIES SUPPORT

The Contractor shall provide the following configuration support services to ITOPS:

1. Provide an information security analysis and documentation to support the implementation of standardized processes, technology configurations, and security controls across VA. Any remediation completed or vulnerabilities identified as a result shall be continuously tracked, monitored, and reported in the Vulnerabilities and Remediation Status Reports and delivered to the COR for review and approval.
2. Provide recommendations, white papers, other documents to enhance ITOPS security processes and documentation. All documentation drafted as a result of these services shall be provided to the COR.

**Deliverables**:

1. Vulnerabilities and Remediation Status Reports
2. Reports, Briefings, and Recommendation Papers

#### ENTERPRISE VULNERABILITY REMEDIATION PLANNING

The Contractor shall provide onsite configuration management support to ITOPS, including:

1. Enhance the monitoring process to identify and communicate changes in systems (e.g., information security controls, configuration baselines) enterprise-wide, and continuously track the status of vulnerabilities in the Vulnerabilities and Remediation Status Report and support communication to the governance board on enterprise-wide vulnerabilities.
2. With input from VA, update the Vulnerability Management Program Plan to define and implement clear roles and responsibilities for developing, maintaining, completing, and reporting vulnerabilities and program strategy, goals, and objectives.
3. Provide reports, briefings, recommendations papers, and other documents to enhance ITOPS security processes and documentation. All documentation drafted as a result of these services shall be provided to the COR.

**Deliverables**:

1. Vulnerabilities and Remediation Status Reports
2. Vulnerability Management Program Plan
3. Reports, Briefings, and Recommendation Papers

#### PATCH AND VULNERABILITY SUPPORT

The Contractor shall provide onsite patch and vulnerability management support to prevent the exploitation of IT vulnerabilities within VA. The Contractor shall perform the following tasks:

1. Manage and maintain the ITOPS’s patch and vulnerability intake process.
2. Collaborate with Office of Information Security (OIS) and ITOPS organizations to streamline the patch and vulnerability management process.
3. Participate in meetings as directed by the COR to further refine and improve processes and procedures for patch and vulnerability management.
4. Coordinate with appropriate groups to manage remediation packages of specific vulnerabilities.
5. Utilize data from ITOPS’ monthly predictive scan results to develop and coordinate completion of appropriate actions and track compliance of baseline implementation.
6. Develop, issue, and manage the VA-approved Patch and Vulnerability Action Item List for change orders and monthly scheduled patch releases.
7. Assist in managing and implementing recurring patches from outside vendors, including Microsoft, Apple, Cisco, and Adobe. Develop a Monthly Patch Report that details the product, patch installed, and date of installation and describes any issues that occurred along with steps taken (if any) to remediate issues.
8. Document and remediate any issues from patch installations and provide Remediation Packages Status Reports.
9. Remediate existing vulnerabilities within system scans, access controls and operating systems/languages within the following timeframes: 40 percent within 3 months, 60 percent within 9 months, and 80 percent within 12 months.
10. Provide new recurring vulnerability remediation.
11. Remediate Windows outliers designated as “OIT ownership” in accordance with the following measure: migrate selected Windows outliers within 7 days of COR/VA PM Assignment (estimated assignment not to exceed 100 per week).
12. Perform an analysis of the TRM process and assist in creating a new process for incorporation into the baseline review/ WAN Impact Assessment.
13. Perform Microsoft patching within 30 days after patch release in accordance with the following measure: 98 percent of all new vulnerabilities identified as approved for remediation by the National Change Control Board (CCB) to be remediated within 30 days.
14. Perform third party patching within 30 days after patch release in accordance with the following measure: 98 percent of all new vulnerabilities identified as approved for remediation by the National CCB to be remediated within 30 days.
15. Remediate 98 percent of all new vulnerabilities within a baseline per month.

**Deliverables:**

1. Patch and Vulnerability Action Item List
2. Monthly Patch Reports
3. Remediation Packages Status Report

#### BASELINE CONFIGURATION PROCESS SUPPORT

The Contractor shall provide product baseline configuration management support to ITOPS and review approved configurations and assist in prioritizing accordingly.

The Contractor shall perform the following tasks:

1. Update and maintain the ITOPS Baseline Configuration Intake process.
2. Provide recommendations to improve the Baseline Configuration Intake process and procedures and deliver a Baseline Configuration Intake Process Recommendations to the COR/VA PM.
3. Review and post new baseline configurations to the ITOPS’s SharePoint site that have been ratified through the WAN Impact Assessment.
4. Assist in the development and submission of action items or bulletins of newly developed baselines developed and ratified by SD.

**Deliverable:**

1. Baseline Configuration Intake Process Recommendations

#### CRISP FIELD OPERATIONS SUPPORT

The Contractor shall provide Continuous Readiness in Information Security Program (CRISP) field operations support services, including:

1. Ensure compliance with standards and guidance set forth by ITOPS.
2. Coordinate efforts across field offices and identify, rationalize, monitor, and control the interdependencies among projects.
3. Manage escalated risks and issues among projects across field offices and consolidate in a Risk and Issues Report.
4. Track and measure the contributions of each field office.
5. Facilitate communication on program status and issues, including attending periodic status report meeting and providing regular status reports to the PM/project manager.
6. Maintain an Integrated Master Schedule (IMS) for the program and critical milestones.
7. Consolidate data across the field offices and develop reports, briefings, and recommendation papers. All documentation drafted as a result of these services shall be provided to the COR.

**Deliverables:**

1. Risks and Issues Report
2. Reports, Briefings, and Recommendation Papers

#### CRISP ONSITE SUPPORT

The Contractor shall provide onsite support and shall have access to the VA authorized help desk and the National Service Desk system for issues or will be assigned action items prioritized by the District Leadership in coordination with the COR. The Contractor will be assigned work covering vulnerability remediation through established national and regional change control documentation systems.

The following Support Tier Levels apply to this PWS:

Level 1 - Identification of incidents, first point of contact; diagnosis, escalation, and resolution based on documented processes and procedures.

Level 2 - First point of escalation; provides guidance and instructions to Level 1 support on diagnosis and resolution. This level takes ownership of incidents where subject matter expertise and experience is required for diagnosis.

Level 3/4 - Change to a component is required for resolution (i.e., code change, hardware replacement, vendor support, etc.).

The Contractor shall provide onsite Tier 2 and Tier 3/4 support at ITOPS facilities to remediate security threats and vulnerabilities in the field. Each region shall achieve a 98 percent or greater remediation rate. The 98 percent or greater remediation rate includes both fixes and creation of Plans of Action and Milestones (POAMs). The severity levels to security threats and the threats backlog will be prioritized and managed by each ITOPS organization. Vulnerability remediation will generally be tracked through the issuance of national action items and in response to the National Patch and Vulnerability compliance expectations; including addressing ITOPS’ identified urgent vulnerabilities, respond to ad-hoc security incident response (emergency patching, updating, and/or sanctioned configuration changes), addressing monthly Microsoft patching requirements, and addressing vulnerabilities discovered from monthly Nessus scanning. Baselines developed will be applied enterprise-wide.

The Contractor shall perform the following:

1. Respond to and resolve tickets and deliver a Ticket Resolution Report that includes the trends of ticket requests, a list of ticket requests, the resolutions proposed, and resolved tickets. The ticketing systems in use are Remedy and Service Desk Manager along with regionally established change control and workload tracking system such as Serena.
2. Implement patches and implement corrective actions needed to mitigate security risks and vulnerabilities and deliver a Patch Implementation Report that includes the list of implemented patches and corrective actions taken to mitigate security risks and vulnerabilities.
3. Support the implementation of IT policies, procedures, and system controls.
4. Deliver a Business Line Issue Report that Identifies any IT-related deficiencies based on scans or other IT assessment tests or techniques.
5. Perform a gap analysis and identify any unresolved tickets or deficiencies. Document the gap analysis in a Gap Analysis Report.

The Contractor shall meet the following service level agreement (SLA) for the Tier 2 and Tier 3/4 support:

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity Code** | **Customer Impact** | **Response to Customer** | **Resolution Goal** |
| **1 – Critical** | Serious consequences resulting in loss of highly sensitive data, functions, equipment/facilities, or the reputation of the VACould impair operations for an indefinite amount of time (e.g., production system unavailable) impacting multiple usersWorkarounds are not in place preventing further impact | 15 minutes | 0-2 business hours |
| **2 – High** | Significant impact to operations (e.g., production system delayed) impacting 1-5 usersWorkarounds may be in place but could severely impact business flow | 1 hour | 2-4 business hours |
| **3 – Medium** | Little impact to continuation of operations (e.g., production and pre-production environments available)Workarounds may be in place preventing further impact | 4 hours | 4-8 business hours |
| **4 – Low** | No impact to continuation of operationsWorkarounds may be in place preventing further impact | 6 hours | 3-5 business days |

Contractors shall comply with an existing Configuration Control Board (CCB) that may exist at the respective Regional areas to track remediation of prioritized vulnerabilities. Remediation responsibilities will be assigned via the work order ticketing system and/or approved change management orders. VA will use established vulnerability compliance performance metrics as outlined in action item issuance, performance measures, policy, and FISMA compliance. Vulnerabilities discovered via monthly predictive scanning shall be patched, removed, or otherwise covered by a risk based decision due to baseline conflict within the days specified in the national monthly Action Item Report.

The Contractor shall include details specific to each VA facility in the Weekly Activity Report.

**Deliverables:**

1. Ticket Resolution Report
2. Patch Implementation Report
3. Business Line Issue Report
4. Gap Analysis Report
5. Plans of Action and Milestones (POAMs)
6. Weekly Activity Report

#### Tier 1 and 2 Onsite Support

The Contractor shall provide onsite desktop technical and security support services on a daily basis during standard hours of operation at sites listed in Attachment 001.

The Contractor shall:

1. Provide workstation, laptop, and printer hardware and software support/troubleshooting, imaging, and patching.
2. Test and image desktops and laptops using Microsoft Operating System Deployment using the VA provided images.
3. Maintain and troubleshoot software and computer peripherals.
4. Set up and configure all workstation, laptop, and printer hardware according to VA standards and baselines.
5. Ensure all open tickets requiring follow-up work and/or calls are resolved within 48 hours. For tickets requiring follow-up work greater than 48 hours as agreed to by COR/VA PM, the severity of the incident shall establish tracking of ticket completion which shall be recorded in the ticketing system.
6. Assist in updating security documents that adapt VA protocols to be in compliance with National Institute for Standards and Technology (NIST) guidelines (e.g., NIST SP 800-53, Revision 4 control families).
7. Use Nessus, CM2012SCOM, and SQL reports and product logs to locate workstations and servers that have inventory, deployment, patching or other issues, and then use provided scripts, tools, and vendor products to troubleshoot and resolve the issue and verify resolution.
8. Build and deploy packages and maintain collections using CM2012.
9. Provide specific vulnerability remediation support for all devices, including laptops, workstations, printers, and network devices (including mobile devices), based on the Regional Director’s priorities, and remediate 98 percent of all new vulnerabilities.
10. Provide onsite or remote as agreed upon by COR/VA PM, patch and vulnerability support using SSCM and other tools. This includes MS patching, Nessus scan remediation, remediation of unauthorized software, baseline image deficiencies, etc. The Contractor support shall include:
11. Analysis of Tenable, Nessus scan results.
12. Vulnerability remediation as required by the Regional Director or designee that cannot be done in an automated fashion according to VA standards.
13. Coordination with stakeholders as needed to remediate the user system or server.
14. Troubleshoot any problems or issues that arise with Windows and Macintosh desktops/laptops from the network drop to the desktop/laptop, prioritizing systems infected with viruses.
15. Troubleshoot any problems or issues that arise with Windows and Macintosh desktops/laptops from the network drop to the desktop/laptop prioritizing systems infected with viruses.
16. Respond to alert notification or escalation of an issue from members of the VA Central Office team, determine the probable cause of the issue, and take the appropriate intervention action(s) to restore the Windows and Macintosh desktop/laptop to operational status.
17. Support Mac Operating System and various Apple tools and applications.
18. Provide operating system updates for Windows and Macintosh desktops/laptops.
19. Provide graphical user interface-level assistance with Mac OS X Server configuration and server administration.

#### Tier 3/4 Onsite Support

The Contractor shall provide onsite, expert technical and security support services and resolve issues that cannot be resolved by Tier 1 and Tier 2 support.

Historically, four (4) to six (6) Tier 4 Subject Matter Experts (SMEs) have been required in each region across each of these areas in addition to the Tier 3 support:

The Contractor shall provide the following support:

1. Workstation administration and patching
2. Server administration and patching
3. Virtualization (VMware or HyperV)
4. Advanced CM2012 (reporting and installing software packages/patches)
5. IBM Endpoint Manager (BigFix)
6. Microsoft Excel fluency, including pivot tables
7. Vulnerability scanning (Nessus or similar)
8. Networking: LAN, WAN, Transfer Control Protocol over Internet Protocol (TCP/IP), Domain Name Service (DNS), Dynamic Host Control Protocol (DHCP), subnets, Classless Inter-Domain Routing (CIDR). Assist both Tier 1 and Tier 2 personnel in resolving vulnerability issues on network systems (routers, switches, etc.).
9. Advanced Active Directory administration and maintenance, domain administration-level experience
10. Database fundamentals (Microsoft Access or SQL Server), including reports and queries
11. Scripting (Microsoft PowerShell preferred)
12. Server imaging, developing standard images, automated deployment
13. Network infrastructure support
14. Resolve network equipment vulnerability issues as outlined by the Regional Director or designee.
15. Work with VA staff on baseline compliance by all regional network equipment.
16. Continuously remediate security deficiencies on VA’s network infrastructure, as identified in Nessus scans.
17. Cisco support with Cisco certified resources and certifications must be kept up-to-date and current.
18. Windows and Linux systems support:
19. Remotely assist both Tier 1 and Tier 2 personnel in resolving vulnerability issues on servers and workstation systems.
	1. Resolve server and desktop vulnerability patching issues for each month’s Microsoft Security Patch Change Orders.
	2. Ensure servers and workstation systems conform to VA baselines.
	3. Remediate and test a solution implemented for specific vulnerabilities as required by the Regional Director or Designee.
	4. Continuously remediate and test solutions implemented for security deficiencies on VA’s network infrastructure, database platforms, and web application servers, as identified by Nessus scans.
20. Use Nessus, CM2012, SCOM, and SQL reports and product logs to locate workstations and servers with inventory, deployment, patching, or other issues; then use provided scripts, tools, and vendor products to troubleshoot and resolve the issues and verify resolutions.
21. Resolve systems management issues related to device security and software configuration.
22. Troubleshoot systems-related issues that impact encryption and device applications.

#### OPERATIONAL PROJECT SUPPORT

The Contractor shall provide project support to ensure proper coordination across ITOPS and with other organizations and timely response (within one business day) to data requests, using the Operational Management Review (OMR) process and general planning activities.

The Contractor shall perform the following tasks:

1. Coordinate and prepare for daily, weekly, and ad hoc meetings, including developing agendas. Provide meeting minutes one business day after meeting.
2. Assist in creating an ITOPS Project Plan that includes the tasking, sub-tasking, work breakdown structure, and coordination of work required for ITOPS to address CRISP actions based on recommendations.
3. Assist in developing a monthly OMR Plan (in compliance with OIS guidance) that includes CRISP OIG recommendations; coordinated input from ITOPS; and tasking, sub-tasking, work breakdown structure, and coordination of work.
4. Manage and organize information collected to describe planned development activities.
5. Provide coordination support between ITOPS and supported customers to manage configuration management reporting requirements and develop Baseline Configuration Reports.
6. Provide recommendations, white papers, other documents to enhance ITOPS’s operation management project processes and documentation.

**Deliverables:**

1. Project Plan
2. OMR Plan
3. Baseline Configuration Reports
4. Reports, Briefings, and Recommendation Papers

#### CONFIGURATION SUPPORT

The Contractor shall provide onsite configuration management support to the ITOPS organization in the execution of its processes to secure the VA IT environment. This includes supporting remediation activities at VA Regional Data Centers, telecommunications, and network operations. Additional tasks include production monitoring of all information systems, production services, and managing the delivery of operations services to all VA geographic locations.

The Contractor shall perform the following tasks:

1. Support creation of and manage new product baselines for network components, including load balancers, Network Access Control (NAC)/port security, software platforms, etc. The Contractor shall document the results in a Compatibility Report.
2. Facilitate site preparation for VA Regional Data Centers, telecommunications, and network operation facilities for OIG audits, including installing software patches and remediating identified vulnerabilities.
3. Provide technical guidance and recommendations to maximize network availability and functionality to ITOPS.
4. Provide vulnerability report monitoring, support, and remediation for network devices, including evaluation of network performance and document vulnerabilities and remediation in a Vulnerability Assessment Report.
5. Perform analysis and diagnosis of highly complex network problems that arise from applying the new network baseline.
6. Update standard templates for configuration baseline, test plans, and implementation/back out plan documents for core technologies listed in Section 5.2.1.11 below. The Contractor shall review the format and layout of the templates with SD for Government approval. During performance, additional configuration baselines, test plans, and implementation/back out plans may be required as infrastructure core technologies may change
7. Update VA-approved Configuration Baseline Template and update Baseline Configuration Standard documents for core technologies listed in Section 5.2.1.11 below. During performance, additional baseline configuration standard documents may be required as infrastructure core technologies may change. The Baseline Configuration Standard documents shall be consistent with VA’s enterprise architecture.
8. Create specifications to address all NIST SP 800-53 security controls appropriate for the system, including:
	1. Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG)s considerations, as appropriate.
	2. Configuration for the information system and its constituent components, including communications and connectivity-related aspects of the system.
	3. Information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device, including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture.
9. Update the VA-approved test plan templates and deliver and maintain updated test plans for the core technologies listed in Section 5.2.1.11 below. During performance, additional test plans may be required as infrastructure core technologies may change. ITOPS has over 400,000 client workstations that use three operating systems (i.e., Linux, UNIX, or Windows) and hundreds of applications to support testing to ensure compatibility. The Contractor is required to document compatibility findings or vulnerabilities in a Compatibility Report. The test plans shall include test cases that sufficiently verify that each specification outlined in the Baseline Configuration Standard document achieves the intended outcome in security posture and system functionality. The test plan shall also include test cases for Functionality Testing, Pre-Production Testing, Limited Scope Production Testing, and Compliance Testing. The test plans shall identify, for Government approval, how and when test reports will be presented and delivered for the various tests.
10. Update VA-approved Implementation/Back out Plan templates and update for the core technologies. During performance, additional implementation/back out plans may be required as infrastructure core technologies may change. The Implementation/Back out Plans shall include the approach, processes, and detailed steps and techniques for uninstalling a new system or component in order to restore a system to its original or earlier state, in the event of failed implementation.
11. The Infrastructure Core technologies consists of the following:
	* 1. WAN
			1. Logical Topology
			2. Border Gateway Protocol (BGP)
			3. Group Encrypted Transport Virtual Private Network (GETVPN)
		2. Wireless Local Area Network (WLAN)/Real-Time Locating Systems (RTLS)
			1. Load Balancing
			2. Firewalls
			3. Network Management/Monitoring
			4. Unified Communications
			5. Video
			6. Windows/Linux
			7. Virtualization
			8. MS Windows Server
			9. VistA Imaging
			10. SQL
			11. Oracle
			12. VistA
			13. Client Workstations
			14. Data Center
			15. Cloud

**Deliverables:**

1. Vulnerability Assessment Report
2. Compatibility Report

#### ENTERPRISE SECURITY AND ANALYSIS SUPPORT

The Contractor shall provide security management and analysis support to ITOPS, utilizing existing datasets from various system dashboards to start trending and analyzing patch and vulnerability remediation efforts throughout VA. Network Enterprise Wellness Tool (NEWT), a central VA-hosted repository shall be enhanced by the Contractor to support analysis efforts and enable reporting to senior leadership.

The Contractor shall perform the following tasks:

1. Monitor dashboards from IBM Endpoint Management (IEM), CM2012, VA’s Governance, Risk, and Compliance tool (GRC) which is used to manage VA’s Assessment and Authorization process, Nessus vulnerability scanner, Nessus security center and the IT Performance Dashboard, Helix Database, QRadar Dashboard, and Computer Associate’s Service Delivery Manager to perform compliance trending and predictive analyses.
2. Recommend best practices in security management, patch and vulnerability management, and configuration management.
3. Utilize monthly bulletins and reports to proactively identify vulnerable systems and deliver ITOPS System Vulnerability Reports and Remediation Plans to address issues, including include trending reports.
4. Coordinate with system owners on a weekly basis to ensure vulnerabilities are valid.
5. Analyze and recommend enhancements to the existing VA-hosted Database Repository Tool to import and manage data sets (e.g., Nessus scans, IEM, CM2012) that can be used for trending and analysis purposes. The Contractor shall manage and maintain the Database Repository Tool in accordance with VIP as required. Prior to any implementation, the Contractor shall require COR/VA PM concurrence on actions.

**Deliverable:**

1. ITOPS System Vulnerability Reports and Remediation Plans

#### INTEGRITY AND AVAILABILITY SUPPORT

The Contractor shall provide configuration management services, including:

1. Analyze vulnerability information, activities, and events that will provide leadership with security situational awareness of the overall security posture in a given District. The analysis shall encompass data analysis and pattern and trend identification that will provide an enterprise awareness of information security risks with solutions that will improve processes of the information security program. The Contractor shall:
2. Review and analyze data from various vulnerability reporting sources to identify trends and provide information on ongoing risks and security situational awareness.
3. Review historical and current data for trends and process improvements in incident response to device infections.
4. Review all current program elements and recommend process improvements that will increase overall security program.
5. Review current incidents and determine appropriate threat levels based on the identification of current risks in the enterprise program.
6. Assist in creating and documenting standard processes by which information security professionals can analyze various vulnerability data, conduct trending and impact analysis, and consult various customers on the meaning of the data and its impact on the enterprise or their Districts.
7. Provide knowledge transfer on the process of conducting impact analysis and vulnerability analysis.
8. Review various existing security data sources such as data from Tivoli Endpoint Manager, Tenable Nessus, Risk Vision, and Solar Winds and provide a recommendation on which data sources would best present an overall security situational awareness for all levels of ITOPS personnel. The Contractor shall:
9. Identify specific reporting metrics to allow for a comprehensive security situational awareness picture based on VA’s unique environment and requirements and industry best practice.
10. Recommend any critical data missing from VA’s various security data.
11. Recommend any process improvements in gathering data.
12. Assist and support implementation of central security situational awareness dashboard improvements within an already established dashboard framework (Microsoft Database, SharePoint), which shall be Section 508 Compliant, and based on the existing NEWT, using the VA Architecture and software standards as referenced in the TRM. In performance, the Contractor shall:
13. Review VA’s various security and operational reporting dashboards for viability as a central security awareness portal for use by Information Security Officers (ISO), Chief Information Officer (CIO), and VA senior leadership.
14. Coordinate acquiring data feeds from current VA security data sources into a central security situational awareness dashboard.
15. Recommend process improvements or data components needed to provide security awareness to ITOPS leadership.
16. Analyze and correlate security data from multiple customers and project leads in order to continuously maintain Security Situation Awareness based in reports for ITOPS Leadership and their customers. The Contractor shall:
17. Maintain contacts with customers through meetings, telephone calls, and other business correspondence to gather data on programs and projects that impact VA’s security posture.
18. Gather data and develop/design appropriate multi-level reporting structures for the program elements to ensure appropriate communication of the current Security Situational Awareness to all levels of the organization.
19. Gather information through interviews and study the procedures and systems currently in place.
20. Prepare security situational awareness reports for customers and stakeholders.
21. Interface with all organizational areas and end users/customers to gather data and analyze ongoing activities for impacts to VA’s security program.
22. Implement VA approved project plans, schedules, and specifications throughout the enterprise.
23. Consult with customers to refine and translate functional requirements into technical specifications.
24. Conduct complex analyses and develop customized reports and queries as necessary to support the program.
25. Analyze incident resolution processes and provide recommendations for improvements to obtain improved efficiency and effectiveness. The Contractor shall:
26. Analyze the current process by which incident resolution communication is handled.
27. Analyze current reporting mechanisms for incident handling.
28. Provided to COR/VA PM for review and approval all reported findings and recommendations before any implementation activities commence.
29. Develop training material and train ISOs and other stakeholders on approved process that may be implemented during performance.
30. On an ongoing basis, review VA POAMs (known as findings in the VA’s Governance, Risk, and Compliance tool) and report on any issues found. The Contractor shall:
31. Prepare reports for COR/VA PM to be used as a tool to communicate findings with VA leadership regarding issues with POAMs.
32. Assist ISOs and other stakeholders in correcting any issues with POAMs.
33. Assist in creating an audit log review process and assist with the implementation of any log monitoring solutions from a Security Officer perspective. The Contractor shall:
34. Analyze minimum auditing requirements and assist in creating a process by which ISOs can effectively and efficiently review audit logs.
35. Document the process and delivery to COR/VA PM that shall at a minimum include:
	1. Specific instructions to field staff.
	2. Reporting capability.
	3. Trending and analysis of the log monitoring reports.
36. Provide technical expertise level support to accomplish the enterprise implementation of a VA enterprise security information and event management (SIEM) product or new audit log processes and procedures.
37. Assist in developing SOPs and enterprise training material in support of the audit log review implementation and its impact and benefits to the field security professionals.

**Deliverables:**

1. Reports, Briefings and Recommendation Papers
2. Standard Operating Procedures

#### VULNERABILITY, DATABASE, AND OPEN VIRTUAL MEMORY SYSTEM (VMS) SCANNING AND ANALYSIS SUPPORT

The Contractor shall provide onsite operational and analytical services in support of the remediation of vulnerability scanning and analysis MWs. ITOPS manages and maintains the VA’s Enterprise Scanning Solution, which is based on Tenable Network Security’s SecurityCenter Continuous View™ and Nessus® scan engines and vulnerability services. Tenable SecurityCenter™ Consoles at the VA District Security Centers rely on more than 265 Nessus scan engines to perform asset and vulnerability discovery and detect system misconfigurations and missing patches for network connected devices in over 1,200 VA facilities.

In performance of the tasks required below, the Contractor may be required to provide support during non-standard hours of operation, including 24/7 operations, as tasks include established scheduled maintenance tasks that cannot be performed during standard hours of operation since minimal interruption of service to VA staff or systems is required. The Contractor shall be required to adjust resource support accordingly as overtime will not be reimbursed to perform established scheduled maintenance occurrences.

The Contractor shall provide operational and analysis support, including:

1. Nessus Scan Data Assessment and Analysis, which includes:
2. Review scan data to determine if the system is performing as designed.
3. Review Security Center/scanner logs for anomalies.
4. Review data in the repositories for scanners that appear to be malfunctioning.
5. Review scan data for trends in vulnerability findings.
6. Review current scan policies and compare with plugins to determine appropriate threat levels.
7. Review current VA security policy and map to Common Configuration Enumeration (CCE) numbers (for compliance scans).
8. Prepare periodic assessment analysis and impact reports as required.
9. Nessus Scan Data Impact Analysis, which includes:
10. Review new vulnerabilities as they are published and develop impact assessments.
11. Determine risk from vulnerabilities based on the following:
	1. Availability of exploit.
	2. Potential loss of information and IT services capabilities.
	3. Number of systems vulnerable to the vulnerability/exploit.
	4. Develop impact assessments for identified vulnerabilities.
12. Prepare periodic trending and impact reports as required.
13. Scan Coordination, Conduct, Reporting, and Maintenance and Management, which includes:
14. Scan Coordination
15. Review and verify Internet Protocol (IP) ranges to be scanned.
16. Review and select appropriate scan policy(s).
17. Coordinate with network and team personnel as required.
18. Scan Conduct
	1. Conduct initial system/data checks upon scan initiation.
	2. Monitor/coordinate/react as required throughout the duration of the scan.
	3. Troubleshoot any issues that occur during the scan.
	4. Verify accuracy of data and conduct system checks as required upon completion of the scan.
19. Scan Reporting
20. Verify report templates.
21. Generate reports.
22. Conduct quality assurance checks of final reports.
23. Distribute reports as required.
24. System Maintenance and Management, which includes:
25. Maintain and manage Government owned enterprise scanning solutions hardware, the Tenable software, and scan analysis and reporting software.
26. Manage and maintain Government owned virtual platforms (VM), operating systems, and applications supporting enterprise scanning solutions.
27. Compliance and Vulnerability Scanning and Data Analysis, which includes:
28. Perform vulnerability scanning against databases for known vulnerabilities, security misconfigurations, and compliance-related concerns.
29. Perform vulnerability scans against Open VMS operating systems. Analyze scan results data and prepare reports for management.
30. Perform penetration tests against various systems, which may include web applications, databases, web services, network devices, operating systems, cloud installations, and infrastructure devices.
31. Provide Compliance and Vulnerability Scanning and Analysis Reports, as required, which shall contain the results of all scans and tests performed on this task.

**Deliverables:**

1. Compliance and Vulnerability Scanning, Trending, and Analysis Reports
2. Enterprise Scanning Solutions Status Reports, Briefings, and Recommendation Papers

### UNAUTHORIZED SOFTWARE SUPPORT

The Contractor shall assist ITOPS in resolving MW’s, findings, and recommendations related to CRISP and unauthorized software, as identified by OIG FISMA audits.

#### SUPPORT FOR UNAUTHORIZED SOFTWARE

The Contractor shall support onsite software remediation tasks for unauthorized and unapproved software, to include analyzing existing processes in monitoring, installing, and removing unauthorized application software on agency devices. Upon completion of analyses, the Contractor shall deliver Briefings and Recommendation Reports. Additionally, the Contractor shall provide Monthly Continuous Monitoring Reports of unauthorized and unapproved software on agency devices on a monthly basis.

**Deliverables:**

1. Briefings, and Recommendation Papers
2. Monthly Continuous Monitoring Reports

#### UNAUTHORIZED SOFTWARE MANAGEMENT AND ANALYSIS

The Contractor shall provide onsite software management and analysis support to ITOPS utilizing the Government owned normalization tool(s) output established by the datasets from enterprise discovery scans. The Contractor shall perform trending and analysis of the software to determine the remediation required for each item.

The Contractor shall use the VA TRM as the baseline authorized software list. The Contractor shall support management and analysis of unauthorized software for inclusion in the TRM or removal from the VA environment. A central VA-hosted repository shall be maintained and updated by the Contractor to support analysis efforts and enable reporting to senior leadership.

The Contractor shall:

1. Recommend best practices in software management, patch and vulnerability management, change management, and configuration management.
2. Review and provide recommendations and updates to the existing Unauthorized Software Standard Operating Procedure(s).
3. Develop incident tickets and submit them to the National Service Desk for execution.
	1. Track tickets as they are being processed through the system and update daily.
	2. Create ticket performance metrics on ticket execution timeline.
4. Perform an analysis on the unauthorized software and determine:
	1. Number of instances of unauthorized software residing in VA enterprise endpoints.
	2. Security status, i.e., number of vulnerabilities associated with each item, if available, using bulletins and security-related data sources and reports to proactively identify vulnerable software
	3. Generate a report of the findings in an Unauthorized Software Status Report and delivery to COR/VA PM for review and approval.
5. Provide the output of the normalization capability to additional consumers in a format that can be ingested into other VA systems.
6. Provide Bi-Weekly Status Reports, which include a trending analysis of remediation efforts.
7. Submit valid identified software items to the TRM for analysis and inclusion.
8. Support onsite management and analysis of unauthorized software for inclusion in the TRM or removal from the VA environment. The Contractor shall:
	1. Assist in creating an SOP by which ISOs will conduct an impact analysis of new, existing, or proposed software to support a determination of whether the software should or should not be used within the VA environment.
	2. Train the ISOs on the existing software impact analysis process.
9. Assist in creating an SOP by which ISOs will conduct an impact analysis of new, existing, or proposed software to support a determination of whether the software should or should not be used within the VA environment.

**Deliverables**:

1. Unauthorized Software Status Reports
2. Bi-Weekly Status Reports

### SYSTEM DEVELOPMENT/CHANGE MANAGEMENT CONTROLS

The Contractor shall provide support services to OIT to resolve the MWs in Change Management and system development controls, as identified by OIG FISMA and FISCAM audits.

The Contractor shall provide change management support services to ITOPS:

1. Assist in developing and/or enhancing change control procedures to ensure the consistent approval and testing during development of system changes for VA financial applications and networks.
2. Review and/or enhance change management procedures to ensure that any changes to system backup procedures are appropriately tested, validated, documented, and approved. Any change management procedures shall be reviewed and approved by COR/VA PM prior to implementation.
3. Provide recommendations, white papers, reports or other documents to enhance OIT’s change management processes and documentation. All documentation drafted as a result of these services shall be provided to the COR.

 **Deliverables:**

1. System Development/Change Management Reports
2. Briefings, and Recommendation Papers

### SYSTEM BACKUP CHANGE MANAGEMENT ANALYSIS

The Contractor shall assist ITOPS in implementing CRISP and system backup/change management recommendations, as identified by OIG FISMA and FISCAM audits..

The Contractor shall review VA Change Management procedures to ensure that any changes to system backup procedures are appropriately tested, validated, documented, and approved. Where deficiencies are identified, recommend improvements and additions to Change Management procedures that address and resolve these deficiencies. The Contractor shall deliver a Change Management Procedures Review and Recommendation Report. Prior to any implementation of change management procedures, the COR/VA PM must approve.

**Deliverable:**

1. Change Management Procedures Review and Recommendation Report

### ACCESS CONTROL SUPPORT

This support is required across all components of OIT in resolving the MWs in Identity Management and Access Controls, as identified by the OIG FISMA and FISCAM audits in this PWS and future FISMA and FISCAM audit recommendations. Additionally, the organizations being supported may be adjusted to reflect the changes resulting from the pending ChooseVA reorganization.

### TWO-FACTOR AUTHENTICATION IMPLEMENTATION SUPPORT

The Contractor shall provide onsite support at any of the VA facilities listed in Attachment 001 to assist in the implementation of a secure, two‑factor authentication (2FA) for authorized user access to VA computing and systems services, to include, CAG. CAG is used with computers and mobile devices not issued by VA as well as VA devices that do not use the Windows operating system.

1. To support 2FA, the Contractor shall:
2. Assist in the engineering, implementation, testing, validation, and administration services for a 2FA system to be used in addition to username/password to provide 2FA during log-in authentication. Prior to implementation the Contractor shall provide a Two-Factor Implementation Technical Plan document.
3. Provide services to assist in the establishment of and maintenance for the applications, services, and other IT infrastructure components to ensure that only those who need access will have access in a two-factor secure method for devices that otherwise will not connect, i.e., non-Windows operating system devices and non-VA issued equipment.
4. Assist in broadening current help desk and support structures to provide adequate user level support from the current user base.
5. Continually monitor the implementation and administration of the 2FA program to ensure a durable design is effectively and perpetually achieving the intended secure access control as a best practice and as required for meeting the FISMA and FISCAM requirement to implement 2FA for remote access to VA. Periodic Performance Reports on frequency and format, including content agreed to by the Government, shall be provided to show progress measures of actual versus target values, percentages achieved, and performance outside of acceptable tolerance levels.
6. Provide reports, briefings, and recommendation papers (such as password and security configuration process(s) enhancements), and other documents to enhance 2FA monitoring and implementation processes and documentation..

**Deliverables:**

1. Two-Factor Implementation Technical Plan
2. Periodic Performance Reports
3. Reports, Briefings, and Recommendation Papers

### INCIDENT RESPONSE AND METRICS SUPPORT

The Contractor shall provide support to assist in resolving the critical weakness, findings and recommendations in incident response and metrics, as identified by the OIG FISMA and FISCAM audits.

#### INCIDENT RESPONSE PLAN AND SOP SUPPORT

The Contractor shall provide onsite support to complete a thorough analysis of existing Incident Response Plan (IRP) and Security Incident Remediation Procedures and deliver an Incident Response Analysis and Recommendation Report to the COR/VA PM documenting deficiencies and gaps within the current IRP and any ineffective and outdated VA incident response policies and processes, incident response procedures, and automated incident response capabilities. When performing this analysis, the Contractor shall consider interactions with other VA SOPs, VA directives and guidance documents, OMB circulars, Executive Orders, existing NIST standards, the United States Computer Emergency Readiness Team (US-CERT) recommendations, and other existing guidance and best practices. In the analysis report, the Contractor shall recommend specific changes and improvements to the IRP and to policies and procedures that address the identified deficiencies. The findings shall be documented and delivered in the Incident Response Analysis and Recommendation Report.

The Contractor shall analyze and update the IRP to include COR‑approved, Contractor recommendations and other COR-required changes and improvements. The updated IRP shall be expanded to address collection, analysis, and archival management of incident response and remediation timeframe metrics and categorization of security incidents in accordance with NIST standards.

As required by the COR, the Contractor shallupdate incident response SOPs, playbooks, and other incident response documentation to align with the updated IRP.

**Deliverable:**

1. Incident Response Analysis and Recommendation Report.

#### MASTER TICKET TRACKING AND METRIC SUPPORT

The Contractor shall complete a thorough review of present Master Ticket procedures plus the findings of any past VA analyses of computer security incident ticketing and reporting. The Contractor’s review shall consider past VA studies and reports on the ticket system and incident remediation reporting processes within VA and its staff organizations, offices, and administrations to ensure that no past metrics information is overlooked. The review shall set the baseline for the VA enterprise processes for gathering metrics on the cradle-to-grave ticket system. The review shall pay particular attention to and with a specific focus on how the VA is tracking the cradle-to-grave reporting of Master Tickets.

During the review and analysis of the ticketing system and metrics program, the Contractor shall document past performance issues, metrics program shortcomings, and best practices for metrics collection and reporting to ensure the tracking system meets VA metrics needs and complies with FISMA requirements and/or all other VA requirements and Federal directives. The Contractor shall deliver Recommendations for Improved Master Tickets Metrics System Report to the COR.

**Deliverable:**

1. Recommendations for Improved Master Tickets Metrics System Report

#### CAT 3 TICKET TRACKING AND METRIC SUPPORT

The Contractor shall complete a thorough review of present CAT 3 Ticket procedures plus the findings of any past VA analyses of CAT 3 computer security incident ticketing and reporting. The Contractor’s review shall consider past VA studies and report on the legacy Remedy ticket system and incident remediation reporting processes within VA and its staff organizations, offices, and administrations to ensure that no past metrics information is lost or overlooked. The review shall set the baseline for the VA enterprise processes for gathering metrics and reporting on CAT 3 tickets.

During the review and analysis of the legacy CAT 3 ticketing system and metrics program, the Contractor shall document past performance issues, metrics program shortcomings, and best practices for metrics collection and reporting to ensure the new tracking system meets VA metrics needs and complies with FISMA requirements and/or all other VA requirements and Federal regulations. The Contractor shall deliver Recommendations for Improved CAT 3 Tickets Metrics System Report to the COR.

**Deliverable:**

1. Recommendations for Improved CAT 3 Tickets Metrics System Report

#### CHILD TICKET TRACKING AND METRIC SUPPORT

The Contractor shall complete a thorough review and analysis of Child Tickets processing from the present Master Tickets system and consider the findings of past VA analyses in reference to ticketing and reporting. The review shall consider past information on the ticket program and processes within VA, including its staff organizations, offices, and administrations, to ensure that no past ticketing metrics information is lost or overlooked. The review shall set the baseline for the VA enterprise for metrics gathering on Child Tickets from the Master Ticket Program, and the Contractor shall pay particular attention to and with a specific focus on how the VA is currently tracking Child Tickets, which includes the remediation methods identified and notification to field organizations, including field response times.

During this review and analysis, the Contractor shall identify past performance issues, capability shortcomings, and best practices for metrics reporting procedures to ensure the new CA-based Child Ticket tracking system meets the federal and legal requirements of FISMA and/or VA and federal government requirements.

The Contractor shall assist in implementing automated Child Tickets metrics collection and reporting in the ticket system.

**Deliverable:**

1. Recommendations for Improved Child Tickets Metrics System Report
	* 1. **SIEM-BASED LOG MONITORING IMPLEMNTATION SUPPORT**

The Contractor shall provide onsite support to assist OIT in resolving MWs, findings and recommendations in Access Control, as identified by the OIG FISMA and FISCAM audits.

The Contractor shall provide onsite technical services required in this task to implement the Government-owned SIEM solution and ensure its integration into VA’s security environments.

The Contractor shall perform the following tasks as part of this support:

1. Assist in developing integration strategies between the SIEM logging solution and other security tools in the enterprise and provide technical support to correlate networked device data feeds with the SIEM logging solution.
2. Provide technical support to activities that require change approval and shall ensure compliance with VA’s strict change control processes, which include technical and security reviews as well as approval and authorization boards. The Contractor’s dedicated onsite SIEM SME shall be integral and engaged with this activity, being required for providing SIEM technical and operational details in order for the approving VA authorities to make informed decisions.
3. Provide on-the-spot SIEM system troubleshooting and provide onsite technical engineering support for production installation in each of the four VA Trusted Internet Connection (TIC) Gateways (GWs).
4. Provide day-to-day operational documentation and support, including enhancing and updating Log Monitoring SOPs, process development, reporting activities, user guides, and operations-related documentation.
5. Assist in developing and maintaining process and procedure documentation for deployment and implementation of the automated audit log solution to each of VA’s five regions and to the VA Data Centers.
6. Provide recommendations for improving the responsiveness of incident categorization and escalation decision-making processes and for the criteria for automated SIEM selection of security incidents and events to be forwarded for analysis and response by Tier 1 analysts. The Contractor shall deliver the results of this analysis as a SIEM Recommendations Report.
7. The Contractor shall provide expert level, technical support to this task which shall include the following:
8. Support with database technologies (Oracle, MS SQL, MySQL, etc.)
9. Support with vulnerability scanning tools (e.g., APPDetective PRO, Point Audit, Tenable, Nessus)
10. Support analyzing and communicating security issues with system administrators
11. Knowledge of common ports and port scanning
12. Support Windows and Unix operating systems
13. Support coordinating and troubleshooting computer/network connection issues
14. Support Microsoft Office and Excel manipulation for logging data and records
15. Provide Command line support (e.g., RedHat, Linux)
16. Ability to create actionable scan reports for a variety of scanning tools

**Deliverable:**

1. SIEM Recommendation Report(s)

## IT OPERATIONS AND SERVICES (T&M)

### FISCAL AND FINANCIAL PLANNING SUPPORT

The Contractor shall provide non-inherently governmental support for Fiscal and Financial planning to support the day to day operations of the organization. The Contractor shall provide surge support for Fiscal and Financial planning, within ITOPS, which includes, but is not limited to, data collection, tracking, reporting, process development and/or implementation of quality assurance checking for the following fiscal areas. (Note: Budget formulation and/or budget planning is NOT part of this task):

a. Critical Funding Needs (CFN)

b. Unfunded Requests (UFR)

c. Budget Tracking Tool (BTT)

d. Multi-year planning (MYP)

As part of the Fiscal and Financial planning support, the Contractor shall:

1. Prepare purchase orders using VA financial systems.
2. Monitor budget execution.
3. Monitor a variety of funding sources (e.g. annual appropriations, construction funding, and franchise fund).
4. Create and monitor Budget Tracking Tool entries.
5. Prepare and provide financial reports to management.

### IMPLEMENTATION MANAGEMENT SUPPORT

The Contractor shall provide Implementation Management services including coordination support across the ITOPS functional areas. The Contractor support shall include coordination with ITOPS personnel and stakeholders for the implementation and sustainment support. The Contractor shall:

1. Facilitate and/or scribe for various meetings related to implementation taskers across ITOPS support organizations.
2. Provide recommendation for both technical and operational requirements and implementation training needs.
3. Review, analyze, and make recommendations for resource requests.
4. Create artifacts associated with implementation such as ITOPS bulletins and action items.
5. Ensure change management and schedule management principles are utilized appropriately.
6. Implement and track key metrics to analyze performance relative to customer service and other key implementation metrics.
7. Utilize and provide SharePoint content management in order to provide resource tracking and information sharing.

### PROJECT MANAGEMENT SUPPORT

The Contractor shall provide project management support for various ITOPS projects and sub-projects. The Contractor shall expedite and coordinate services to assist in managing complex enterprise projects. The Contractor shall manage assigned tasks to completion within the schedule, budget, and scope of the individual project. The Contractor shall ensure objectives of the projects are achieved, as defined by VA.

The Contractor shall:

1. Conduct all aspects of project initiation, planning, execution and closeout per industry standards and guidelines established for Project Management Professional (PMP) certification.
2. Follow VA and ITOPS standards and procedures for Project Management.
3. Develop formal project charters as required by the ITOPS PM.
4. Facilitate project kick-off and status meetings and communicate individual roles and project expectations.
5. Conduct formal project reviews with project sponsor at project completion.
6. Conduct reviews with the VA PM on a periodic basis.
7. Keep the VA PM, customer, and project team informed of the status of the project being managed.
8. Coordinate activities with existing ITOPS customers.
9. Coordinate activities for ad hoc requests from internal and external customers.
10. Develop and maintain detailed project plans and WBS of the tasks required to execute the project.
11. Develop Project Schedules that are deliverables-based and accurately depict the work to be performed by the project. The Contractor shall ensure all project plans, WBS and schedule work products are retrievable by the COR/VA PM(s) for any reviews and approvals required.
12. Monitor project milestones and critical dates to identify potential jeopardy of project schedule, and identify ways to resolve schedule issues.
13. Ensure that risks associated with the cost, resource, schedule, and technical aspects of the project are identified, assessed, documented, tracked, and mitigated. The Contractor shall ensure all issues tracked are accessible by the COR/VA PM(s) for any reviews and approvals required.
14. Notify VA management of issues that impact the project and require management decisions.
15. Develop system development plans, track activities to the plan, and communicate status, utilizing the latest ITOPS Project Management tools.
16. Assess variances from the project plan, and develop and implement changes as necessary to ensure project remains within specified scope as well as time, cost and quality objectives. The Contractor shall ensure all variances tracked are accessible by the COR/VA PM(s) for any reviews and approvals required.
17. Maintain a collaborative environment with key stakeholders(s).
18. Participate in the development of project standards, procedures and quality objectives. The Contractor shall utilize industry and ITOPS established project standards, procedures and quality objectives without requiring assistance from others. All documentation shall be provided to the COR/VA PM for approval prior to any implementation or changes.
19. Identify artifacts needed to establish and maintain control of the project. Create and utilize those artifacts mandated by VA and ITOPS standards.
20. Communicate assigned responsibilities to project members for developing artifacts and performing project activities.
21. Review project management activities with VA Senior Management on a periodic basis.
22. Review project-planning activities with the Project Team on a periodic and event-driven basis.
23. Develop estimates for project’s effort, costs, and critical computer resources according to the specific application.
24. Notify all affected groups of approved change orders.
25. Track effort, cost, critical computer resources, development activities, and schedule, and take corrective actions as necessary.
26. Make and use measurements to determine the status of planning, tracking, and oversight activities.

### ADMINISTRATION AND CLERICAL SUPPORT

The Contractor shall provide support to the ITOPS Service offices with support for tasks such as: time keeping activities, monitoring service e-mailbox; distribution of mail, both paper and e-mail; developing travel and training documents; and setting up, attending and documenting meetings.

The Contractor shall perform the following:

1. Time keeping activities, completed in accordance with the ITOPS administrative processes
2. Review timecards that cannot be processed because of inaccuracies due to typos or incorrect timecard entry; if required, the Contractor shall contact the employee or the employee's supervisor to resolve. The Contractor shall perform daily research and correction of discrepancies for employees.
3. Facilitate and schedule appointments, coordinate meetings and reserve conference space for personnel, as well as performing meeting set-up and other coordination activities. New, recurring, rescheduling or cancellation of meetings and/or appointments shall be scheduled the same day the request is received.
4. Prepare interoffice/executive correspondence and maintain administrative filing system for the Service with an internal administrative control.
5. Prepare and maintain operating and desk procedures, methods, standards, policy memoranda and techniques concerning administrative procedures within the Service, and recommend required changes and adjustment to assure proper and accomplishment of Service goals and objectives.
6. Maintain the Service e-mail box by taking action on each message.
7. Prepare, edit and/or conduct reviews for recurring and one-time reports, suspense items, date sensitive actions and correspondence required for the various functions of the Service. The Contractor shall ensure final documents are routed or mailed to the designated source(s) after receipt of all required concurrences/approvals.
8. Answer the telephone, take messages, respond to routine inquiries, and direct calls to staff. Copy, bind, and collate documents and ensure distribution and mailing.
9. Assist with the preparation of travel documents to include preparing the travel request, estimate and justifications. The travel request will be finalized by VA employees after all steps have been taken. Upon completion of travel, the Contractor shall assist with completion of the travel voucher to include: mileage calculation, adherence to proper format, obtaining appropriate finance and supervisor's approval. The travel voucher will be finalized by VA employees after all steps have been taken.
10. Obtain and monitor the use of services/supplies for the Service. The Contractor shall track office supplies, gathering requests for office supplies, answering questions concerning policies and procedures related to office supply services. The Contractor shall coordinate the needs of subordinate offices and coordinate tracking requests for office supplies to meet the office's needs.
11. Prepare supply reports, correspondence and fact sheets for use by the Service in support of decision making.

### TECHNICAL DOCUMENTATION SUPPORT

The Contractor shall provide technical writing support to address emerging requirements and in support of additional ITOPS Service offices.

The Contractor shall:

1. Provide written and verbal communication support while utilizing effective prioritization and multi-tasking skills in the fast paced environment. The support provided shall include a wide variety of technical and administrative topics and require the Contractor to have the ability to quickly grasp a variety of concepts and explain them clearly and concisely in written form.
2. Edit, standardize, and/or make changes to material prepared by other writers, to create error-free, publishable documents in adherence with the Associated Press (AP) Stylebook and VA Public Affairs Guidelines.
3. Create templates; edit and format reports, charts, tables, and presentations utilizing the Microsoft Suite and Adobe Professional.
4. Use Visio to create complex workflow diagrams, process maps, and process models.
5. Lead process owners in discussions to develop documentation supporting ITOPS work products.
6. Create and maintain SharePoint workflow processes integrated with MS Outlook.
7. Utilize SharePoint to create and configure sub-sites, lists, libraries, permissions, features, and manage versioning.
8. Provide meeting scheduling, facilitation, and note taking support as needed.

### BUSINESS PROCESS SUPPORT

The Contractor shall provide business process support for ITOPS Service offices creating, monitoring, re-engineering and documenting critical business processes.

The Contractor shall:

1. Provide analysis of IT business and information processes, activities, and events.
2. Provide analysis of data processes, process trends, and patterns to identify risks and opportunities for increased efficiencies.
3. Provide recommendations that offer solutions for improving ITOPS business processes
4. Prepare agreements (i.e Service Level Agreements (SLA), Organization Level Agreements (OLA)), modifications, rough order of magnitude estimates, and other business documents.
5. Continually monitor agreements and projections, including researching variances and documenting revised projections in monthly variance reports.
6. Research and respond to customer inquiries regarding business agreements, documents, and other business related matters as necessary.
7. Gather and analyze data for annual business planning processes.
8. Provide/report timely and accurate status updates for assigned tasks.
9. Participate in special projects related to business process efforts.
10. Perform processes analyses to define opportunities for new or improved business process solutions. Any recommendations shall be provided to the COR and VA PM(s) prior to any implementation or changes.
11. Conduct Gap Analyses for ITOPS business process engineering.
12. Conduct Feasibility Studies and Trade-off Analyses.
13. Prepare business cases for the application of IT solutions.
14. Present information formally and informally, including business cases, best practices recommendations, process designs, briefings and training to a variety of audiences as coordinated with the COR and VA PM
15. Use the standard ITOPS change management system to obtain new work assignments, update status and store work products as necessary.

**Deliverable:**

1. Gap Analyses
2. Feasibility Study
3. Trade-off Analyses

### SHAREPOINT MANAGEMENT SUPPORT

#### SHAREPOINT ADMINISTRATION SUPPORT

The Contractor shall have functional knowledge of Microsoft SharePoint Server (MOSS) 2007 and 2010 (SharePoint) application and infrastructure components. The Contractor shall assess and facilitate product strategies between MOSS 2007 and 2010, Windows SharePoint Server (WSS) 3.0, and Microsoft Office Forms Server 2007. The Contractor shall conduct architectural design, web parts development, VA server installation, management and troubleshooting with focus on planning, deploying, and supporting SharePoint implementations.

The Contractor shall:

1. Act as the SME for SharePoint 2007-2010
2. Provide technical and architectural expertise to SharePoint developers and administrators.
3. Work with site collection stakeholders and site content managers to create/build SharePoint solutions and migration support.
4. Lead architecture and process strategies, ensuring that the enterprise SharePoint environment is scalable, sustains performance requirements, and complies with VA’s privacy and security policies. All recommended strategies shall be provided to the COR/VA PM(s) for approval prior to any implementation or changes.
5. Monitor and respond to escalated Service Desk tickets, supporting SharePoint technicians and Interns as required.
6. Develop course content and conduct training for SharePoint.
7. Implement and support “form services”, custom reporting, custom workflow, and searches.

#### CONTENT MANAGEMENT SUPPORT

The Contractor shall provide SharePoint content support by answering phone calls, e-mails, service requests, and maintaining a public knowledge base for web related questions, and web content related issues (e.g., FAQ repository). The Contractor content management support shall provide functional knowledge of MOSS 2007 and 2010 (SharePoint) application and infrastructure components.

 The Contractor shall:

1. Respond to content requests including streaming media (audio/video), permission requests, SQL support, new website or application requests.
2. Setup new web sites on VA Internet, Intranet and/or development servers in accordance with ITOPS Site Build Process procedures and the VA Web Application Request Procedure.
3. Perform activities associated with determining and documenting the new site requirements, permissions, compliance with policy and standards including VA 6102 Handbook “*VA Directive Internet / Intranet Services*” and providing initial site template guidance are included in this task.
4. Perform troubleshooting and restoration services to sustain the functionality for ITOPS.

### SECURITY ADMINISTRATION SUPPORT

#### Security Analysis Support

The Contractor shall provide Information Security support which includes the following tasks:

1. Analyze vulnerability information, activities, and events and provide leadership with security situational awareness of the overall security posture. The analysis shall encompass security data analysis, and pattern and trend identification to provide an enterprise awareness of information security risks with recommended solutions to improve processes of the information security program.
2. Review various existing security data sources that include but are not limited to data from Tenable, Nessus, Risk Vision, and Solar Winds and provide a recommendation on which data sources would best present an overall security situational awareness for all levels of personnel. The Contractor shall support the implementation of approved security tools, promulgation of security requirements, and automated processes utilized to report system statuses, data integrity, customer service levels, and other information.
3. Analyze security incident resolution processes and provide recommendations for improvements to obtain improved efficiency and effectiveness. Assist in audit log review processes and implementation of any log monitoring solutions
4. Assist in creating and documenting standard processes by which information security professionals can analyze various vulnerability data, conduct trending and impact analysis, and consult various customers on the meaning of the data and its impact on the enterprise areas of responsibility.
5. With input from VA, create security audit review processes and assist with the implementation of any continuous monitoring requirements and solutions from a Security Officer perspective.
6. Assist in developing SOPs and enterprise training material in support of security auditing, POAM reviews, Authorization to Operate (ATO) processes, and Assessment and Authorization, and report the impact and benefits to the field security professionals.
7. Train information security professionals on the process of conducting impact assessments and analysis, reviewing POAMs, vulnerability scanning and analysis, and remediation.
8. Develop training material and train stakeholders on approved security processes and procedures that may be implemented during performance.
	1. Analyze minimum auditing requirements and assist in creating a process by which Information Security staff can effectively and efficiently review audit logs.
	2. Develop SOPs and enterprise training material in support of the audit log review implementation and its impact and benefits to the field security professionals.
9. Support the implementation and maintenance of Technical, administrative, and physical security controls and associated security evidence and artifacts to address the MW as identified by the OIG FISMA and FISCAM audits and future FISMA and FISCAM audit recommendations.

#### CLOUD SECURITY SUPPORT SERVICES

The Contractor shall provide technical and security support, including:

1. Performing qualitative assessments of current cloud computing frameworks particularly as it relates to security in cloud environments.
2. Creating an Assessment Report (Cloud Implementation Assessment Report) based on the qualitative assessment, documenting detailed recommendations of cloud-based, on-demand, scalable, secure, and reliable computer services, considering options such as Infrastructure as a Service (IaaS), Software as a Service, (SaaS), Platform as a Service (PaaS) cloud computing stack options, etc.
3. Outlining recommendations for security process creation and changes necessitated by the move to a cloud-based service structure.
4. Creating, implementing, and upkeep of standard operating procedures (Cloud Security Standard Operating Procedures), guidelines, and guidance pertaining to secure cloud implementations, migrations, and sustainment.

**Deliverable:**

1. Cloud Implementation Assessment Report

#### Infrastructure Security Support

The Contractor shall provide support including:

1. Provide security support for all components of security operations and sustainment related to vulnerability management, inventory management, systems, networks, isolation architecture, applications, software, medical devices, and specialized device support to include assessment and authorization, risk management, incident response, continuous monitoring and readiness management, and audit support.
2. Provide support for the implementation and sustainment of the Enterprise strategies for Risk Management Framework and lifecycle management for medical devices, special purpose systems, and applications to include the procurement and installation of medical devices and special purpose systems through decommissioning and disposal.

#### CYBERSECURITY TRAINING

The Contractor shall coordinate with government teams to deliver, monitor, and track existing Cybersecurity, Information System Security Management, and Information System Security Management training. The Contractor shall review, update, establish, track, and report Standard Operating Procedures and communicate Enterprise Standard Operating Procedures and Security documentation to cybersecurity personnel.

### APPLICATION MONITORING SUPPORT

The Contractor shall provide code level support for applications, scripts, and middleware software, including code review, testing, debugging and patching, as well as error correction, defect repair and training of applications. The Contractor shall configure and install upgrades/patches to provide software per maintenance agreements, using change and release management processes.

The Contractor shall:

* 1. Perform requirements analysis for new application features, analysis of current system capabilities and limitations and design/engineer/integrate new system capabilities to meet requirements in an architect capacity only.
	2. Provide SME support to monitor and analyze application performance, desktop performance, and availability monitoring/reporting using available tools such as CA Application Performance Management, AppDynamics monitoring tools, Arcturus Applicare, Microsoft Bluestripe Factfinder, XPOlog Management, CA Service Operations Insight, CA Business Service Insight, Aternity Desktop monitoring, and other performance monitoring tools as required.
	3. Customize the monitoring interface to provide dashboards, monitoring and alerts for numerous applications in the production and pre-production environments.
	4. Document and test the interface customizations.
	5. Provide knowledge transfer training to Government and Contractor development and performance testing support staff personnel on the use of the monitoring diagnostic tools to find the root cause(s) of performance issues.
	6. Provide knowledge transfer training to Government and Contractor helpdesk staff and Information Technology Specialist (ITS ) staff on the use of monitoring diagnostic tools to pinpoint production issues.
	7. Provide knowledge transfer training for Government and Contractor development staff on Root Cause Analysis based on data reported from the monitoring system.
	8. Create and refine performance monitoring and availability alerts.
	9. Recommend policies and procedures on actions to take based on the alerts generated. All recommendations shall be provided to the COR and VA PM(s) prior to any implementation or changes.
	10. Provide subject matter expertise to recommend standards, policies and procedures related to the use of application performance monitoring and availability in the pre-production and production environments. All recommendations shall be provided to the COR/VA PM(s) prior to any implementation or changes.
	11. Provide subject matter expertise to evaluate and refine system monitoring efforts.
	12. Provide customer support to resolve performance issues.
	13. Monitor subsystems using customized scripting appropriate to the monitoring tool being used.
	14. Document operational steps and practices necessary to perform the assigned monitoring duties.

### NETWORK AND INFRASTRUCTURE MONITORING SUPPORT

The Contractor shall:

* 1. Perform analysis for performance monitoring of new network and infrastructure system features, current system capabilities and limitations in order to meet ITOPS monitoring metrics.
	2. Integrate network and infrastructure monitoring tools with other monitoring systems and reporting dashboard tools.
	3. Provide SME level support on network and infrastructure monitoring tools such as CA Spectrum Infrastructure Manager, CA Service Operations Insight, and CA Virtual Assurance, CA Unified Infrastructure Management, Orion Solarwinds, CA eHealth, CA NetQoS and other similar system management tools.
	4. Provide knowledge transfer to Enterprise Service Desk, IT, and performance testing staff on the use of the network and infrastructure performance monitoring and availability systems in order to increase efficiency diagnosing the root cause of performance issues.
	5. Assist in developing standards, policies and procedures for the use of network and infrastructure performance monitoring and availability suite of products in the pre-production and production environments. All recommendations shall be provided to the COR and VA PM(s) prior to implementation or changes.
	6. Participate in refining and troubleshooting efforts.
	7. Provide customer support to resolve identified performance issues.
	8. Adhere to all ITOPS IO program and naming standards.
	9. Support, install, configure, and perform fault isolation for server migration/OS upgrades. The migration/upgrade shall be accomplished within approved timelines and with no significant user impact.

### SYSTEM ADMINISTRATION SUPPORT

The Contractor shall provide system administration support to operational servers, desktops, and laptops in multiple environments (production, staging/test, and development, as available) in support of the VA system. When administering Government owned or leased equipment, the Contractor shall ensure its personnel have proper security clearance, full familiarity with operation processes and procedures, and full compliance with site specific regulations, processes and procedures.

The Contractor shall:

1. Prepare, implement and update an Operations and Maintenance Plan in accordance with VA IT policies and procedures.
2. Perform the following system administration functions:
3. Server Provisioning
4. Operating System Installation
5. Install OS Patch Installation
6. OS Patch removal (if applicable)
7. OS Upgrades
8. OS and hardware Troubleshooting (HW) issues
9. Input/Output (I/O) device configuration
10. Create, configure, mount, grow, and maintain file systems / file shares
11. Install Commercially Available Off-the-Shelf (COTS) software (SW)
12. COTS SW Patching
13. COTS SW Upgrades
14. Manage local user accounts in accordance with VA Policy.
15. Validate, create, and maintain system documentation, logging changes that occur as a result of system fixes, system changes, enhancements and expansions. The Contractor shall provide written recommendations to the Government on existing systems to ensure they are in compliance with all Federal requirements and meet industry best practices.
16. Manage system licenses, including keeping a log of license expiration periods, notifying the COR not later than 90 days prior to each expiration.
17. Collaborate with project teams; security, database and network administrators, ISOs, operations support staff, stakeholders, including Department of Defense (DoD) operations, and other system administration support staff.
18. Assure that all routine hardware and software upgrades are performed in a timely manner and documented in maintenance logs concurrent with the actual maintenance being performed.
19. Utilize log data and system administration tools to diagnose system hardware and software problems, repair, and re-configure or replace defective system components as indicated.
20. Perform system monitoring and analysis on assigned systems to discover risks and inadequacies, and provide recommendations on the need for expansion, enhancement or revision.
21. Ensure that system backups are scheduled and performed in accordance with the Operations and Maintenance Plan. The Contractor shall provide for the restoration of backups, files and databases as needed to restore system availability in the event of hardware, security, or administration failure. The Contractor shall also log backups in System Maintenance Logs concurrent with the performance of this action.
22. Perform routine audits of systems and software to determine utilization and adequacy for demand, and compliance with current hardware and software site license regulations and requirements.
23. All system logs shall be logged to the defined loghost. The Contractor shall ensure local logs are used for troubleshooting purposes only and rotated to avoid logging issues and allow for removal to avoid running out of disk space on system disks.
24. Where system failures occur and cause system downtime, the Contractor shall:
25. Notify the Enterprise Service Desk immediately. After notifying the service desk, the Contractor shall notify the system owner and the application team, and provide a brief description of the known situation. Notification may occur by telephone, but shall also occur by email with a subject line that reads: NOTIFICATION OF SYSTEM DOWN.
26. Provide updates to the Incident Commander at least every two hours until resolution.
27. Following resolution, provide a System Failure Lessons Learned Report which identifies the root cause of the problem, clearly specifying if the outage was a result of facility resource availability, product hardware failure, product software failure, process issue, or human error. This report shall be provided to the Problem Management team following the Incident follow up. The System Failure Lessons Learned Report shall identify the proposed approach for preventing a repeat of the outage.
28. Implement automation capabilities using existing VA configuration management, scheduling, and orchestration tool sets (i.e.: CM2012, SCOM, Puppet, BigFix, Ansible, Control-M, CA-7 Scheduling, CA Workload Automation, etc.) to improve, streamline system administration tasks and processes.
29. Assist on system administration process improvement teams. Design, document, and provide knowledge transfer as needed.

**Deliverable:**

1. System Failure Lessons Learned Report

### PLATFORMS AND STORAGE SUPPORT

The Contractor shall provide server and storage support services for ITOPS support locations. The Contractor shall provide onsite system administration support for the VA Hypervisor environment, Microsoft or Linux, and other OS platforms, to include their hardware from various manufacturers throughout the Enterprise. The Contractor shall conduct the following tasks, and also provide all tools required in support of these areas:

1. Test and apply server Basic Input/Output System (BIOS) and firmware upgrades within deadlines established by VA, approximately quarterly.  Document upgrades within existing Change Management system.
2. Install, deploy, configure, and update servers within established VA baselines.
3. Update documentation, (Change Orders, rack elevation diagrams, procedures and logs) within one business day after adding, moving, or excessing (i.e. removing) hardware equipment within the data center.
4. Troubleshoot and resolve Help Desk tickets.

The Contractor shall provide onsite system administration support for the VA Storage environment. The Contractor shall administer data storage technologies, replication and backups for converged Storage Area Network (SAN) and /or Network-Addressable Storage (NAS), Common Internet File System (SUN); Common Internet File Services (Microsoft) (CIFS), Network File System (NFS), File and Block storage, Fiber Channel, and Backup systems.

### SYSTEMS QUALITY CONTROL SUPPORT

The Contractor shall provide a System Test Plan for assigned efforts. The Test Plan shall include a Test Schedule and outline the test approach and planned activities for the performance testing required for assigned efforts. Specifically, the Contractor shall develop, in conjunction with business and technical stakeholders, the Test Plans and Test Schedule documenting the relative mix of use cases and their frequency of execution. The Contractor shall analyze and conduct performance testing of software and hardware changes and upgrades, after they are implemented by the Government into the performance testing environment, prior to production deployment to ensure the changes and upgrades do not cause unacceptable performance degradation.

The Contractor shall

1. Utilize the CMM methodology and ITOPS testing procedures.
2. Facilitate, document and provide subject matter expertise in project meetings, regarding testing efforts.
3. Verify projects are unit, system and regression tested.
4. Develop System Test documentation and reports according to ITOPS methods and deliver them to COR and VA PM.
5. Conduct risk assessments of systems and/or programs assigned to support testing.
6. Develop system test estimates, schedules, objectives, and cases.
7. Collect internal, project and customer-defined metrics for testing.
8. Design and prioritize System test plans, test cases, and test scripts.
9. Execute assigned test plans, test cases, and test scripts.
10. Enter defects into the VA defect tracking systems.
11. Retest resolved defects on each release.
12. Conduct all system test activities in accordance with project schedules.
13. Provide status of all system test deliverables to COR and VA PM as required.
14. Conduct required reviews and audits and submit the results in accordance with established procedures to COR and VA PM. These should include: Technical and Product Reviews, Peer Reviews, Process Audits, Risk Assessments, Earned Value Analysis, and metrics reports.
15. Prepare all plans, reports, schedules and findings according to CMM methodology.
16. Research and analyze the information contained in the findings to ensure the work products meet test criteria.

**Deliverable:**

1. System Test Report
2. System Test Plan
3. System Test Case

### DOMAIN INFRASTRUCTURE SUPPORT

The Contractor shall provide services related to all types of domain infrastructure support and services and Public Key Infrastructure (PKI) certificate management. The Contractor shall provide support services expertise in domain infrastructure products, utilization, implementation, reporting metrics, and report development.

1. Active Directory Management to include:
	1. Group Policy Management
	2. Access Management using tools such as Active Directory Users and Computers (ADUCs) and Forefront Identity Managers (FIM) to manage Users and Group membership.
	3. Elevated Privileges approval and implementation.
	4. Domain Name Services (DNS) Management
2. Service Now ticket routing, troubleshooting and remediation.
3. Continuous Readiness in Information Security Program (CRISP) Reviews and Remediation:
	1. Elevated Privileges review and remediation.
	2. USGCB Compliance
	3. Audit Preparation and Reviews.
4. Centrify Management (Active Directory support for Apple Macintosh & Xnix systems.)
5. Scripting solutions for automation and reporting.
6. PKI Certificate Management to include:
	1. Manage PKI Certificates throughout the Enterprise
	2. Conduct an Enterprise level inventory of all PKI certificates
	3. Establish and maintain a timetable that addresses expiring certificates for renewal, change, or elimination
	4. Obtain and process new certificates
	5. Ensure processes and procedures are Enterprise level to cover 100% of all PKI Certificates

### SYSTEMS ROUTINE MAINTENANCE SUPPORT

The Contractor shall conduct routine maintenance planning in coordination with VA PMs and project managers as well as site operations managers and administrators. The Contractor shall deliver a detailed Routine Maintenance Schedule that identifies routine maintenance activities by system and site. The Contractor shall conduct routine maintenance on designated IT systems, system components, or other products using maintenance and administration manuals provided as Government Furnished Information (GFI) and in accordance with the COR approved Routine Maintenance Schedule. This shall include coordination with system administrators to coordinate maintenance activities with specific site schedules. The Contractor shall notify the system administrator of any required down-time at least seven (7) calendar days prior to the planned event and shall coordinate required down-time to ensure the least possible impact to VA operations.

The Contractor shall provide routine maintenance to include providing help desk services to end users of the system, subsystem, or component. In performance of these services, the Contractor shall provide routine maintenance support which includes:

1. Maintenance service, five (5) days per week, Monday through Friday, during the hours of 8:00 AM – 5:00 PM Local time.
2. After hours support, as needed.
3. Analysis to identify trends, system bugs, and deficiencies.

**Deliverable:**

1. Routine Maintenance Schedule

### CONFIGURATION MANAGEMENT (CM) SUPPORT

The Contractor shall provide configuration management support at the ITIL program office level and support the ITIL function of configuration management, as it is executed throughout OIT. The ITIL program, Service Asset Configuration Management ensures that the service assets and Configuration Items (CIs), upon which IT services are relying, are properly monitored; information regarding the configuration of those service assets and CIs is accurate; and the relationships between them is available anytime, anywhere.

The Contractor shall support the design and implementation of formal procedures, including checks and balances throughout the CM process. The Contractor shall identify and mitigate risks to ensure the integrity and recoverability of the production environment and ensure the currency, accuracy, and completeness of the Configuration Management Database (CMDB) for all OIT business services, applications and infrastructure. The Contractor shall provide support to ensure that only authorized components specified within the approved toolset and change management process, as referenced in National Directive 6004, referred to as CIs, are used in the IT environment. The Contractor shall record, track and audit all changes to CIs throughout the component’s life cycle. The Contractor shall support lifecycle management and configuration management for services, hardware and software systems. The Contractor shall practice sound data management strategies, utilize analysis methodologies to determine viability of systems and be able to report and document issues.

The Contractor shall:

1. Comply with OIT Service Asset Configuration Management (SACM) policies and procedures.

2. Define the structure of the CM system, including CI types, naming conventions, attributes and relationships. The Contractor shall identify the data sources for CI population, and identify and review the configuration data model requirements.

3. Implement the Configuration Data Model in the ITSM Tool.

4. Update the CMDB with new CI information and status information.

5. Maintain quality of CI information entered into ITOPS IO CI Databases.

6. Perform verification and audit of CMDB.

7. Perform and document software and hardware baselines.

8. Work with managers, Senior Configuration/Data Management Analysts, software/hardware engineers, and other software/hardware development specialists to ensure approved CM processes and quality assurance procedures are incorporated.

9. Make changes to the CI Class structure as required.

10. Incorporate appropriate security testing in the CM processes and quality assurance process.

11. As requested, provide information and reports to management relating to CM procedures.

12. Submit Change Orders for changes to production systems, as needed.

13. Conduct and document software and hardware inventories.

14. Provide support in the event of system outages or disasters.

15. Participate in configuration control board(s).

16. Work with Change Manager to facilitate Emergency Changes.

18. Review CI update requests and respond to requests for CI changes and updates.

19. Create, validate and Update Configuration Record.

20. Support the SACM program owner and SACM Process Manager in the creation of principles, processes and procedures.

21. Work closely with CM to analyze changes and ensure CMDB is updated.

22. Escalate to the Change and SACM Process Manager any unauthorized CI changes or alterations to environment not reflected in CMDB.

23. Support effective use of CMDB by participating in support groups and other processes.

24. Assist SACM Program Manager in conducting configuration audits and reconciliation.

25. Produce and analyze reports related to the SACM process.

26. Identify and recommend process and procedure improvements.

27. Train staff in CM principles, processes and procedures.

28. Control the receipt, identification, storage and withdrawal of all supported CIs.

29. Maintain and provide status information on Cis.

32. Identify, record, and distribute SACM issues.34. Assist ITOPS in planning for CMDB’s and activities.

35. Provide management information about CM quality and operations

37. Comply with VA and ITOPS IO security and privacy policies and directives, and CRISP. The Contractor shall take immediate action and ensure resolution of violations and non-compliance in regards to ITOPS IO and VA policies, procedures, directives, and management handbooks.

38. Report violations and non-compliance to COR and VA PM(s) as required.

### CHANGE MANAGEMENT SUPPORT

The Contractor shall provide change management support at the ITIL program office level and support the ITIL function of change management, as it is executed throughout OIT. The ITIL change management aims to ensure that standard processes and procedures are used throughout OIT to deploy changes in a controlled manner. This ensures the integrity of the production infrastructure through the effective application of change management processes and management techniques that ensure a Request for Change (RFC) is planned, scheduled, reviewed, implemented and closed in a standardized manner. The Contractor shall review, analyze and standardize change processes and audit those processes as well. The Contractor shall support the design and implementation of formal procedures, including checks and balances throughout the process. The Contractor shall identify and mitigate risks to ensure the integrity and recoverability of the production environment and ensure the currency, accuracy, and completeness of the CMDB for all business and technical data elements for ITOPS applications.

The Contractor shall:

1. Comply with OIT change management policies and procedures.
2. Plan and execute RFCs.
3. Identify tasks and coordinate with deployment teams for RFCs.
4. Assist with issues regarding coordination and approval of changes as necessary.
5. Communicate RFC approval/rejection to service recipients.
6. Monitor change deployment and ensure notification and escalation activities.
7. Review implemented changes to ensure that they have met their objectives.
8. Verify the success of the install and initiate or request a back out/restore in case of failure.
9. Participate in Post Implementation Review (PIR) when required.
10. Perform and complete actions assigned at the PIR/Assessment.
11. Update RFC with implementation details and assigns ‘completion code’, where appropriate.
12. Attend Change Advisory Board (CAB) meetings where applicable.
13. Communicate the RFC implementation at technical meetings.
14. Ensure required documentation is provided in the RFC.
15. Ensure that CI attribute updates are accurately reflected in the RFC.
16. Review plans for RFC (e.g., Implementation Plan, Test Plans/Test Results, Back-Out Plans, Resource requirements).
17. Review RFCs for categorization, urgency, impact, priority, risk, impact and completeness.
18. Schedule RFC implementation and resolves schedule conflicts.
19. Approve changes within their area of responsibility and refers changes affecting other areas to the CAB for approval.
20. Develop, distribute, and review change reports to ensure process adherence, monitor trends and address areas of concern.
21. Audit planned changes for accuracy and completeness of all components to include preparation, execution, and testing.
22. Audit and report status of changes across the enterprise.
23. Produce and distribute regular and monthly report on RFC Statistics to stakeholders.
24. Coordinate and determine when to schedule a change, integrate new and scheduled changes into a consolidated Forward Schedule of Change (FSC).
25. Determine CAB meeting attendees, depending on the nature of the RFC, and areas of expertise. The Contractor shall convene CAB meetings for all urgent RFCs.
26. Chair the CAB as needed.
27. Complete actions assigned at the CAB meeting, which may include actions for approval criteria if contingent approval is granted to an RFC at the CAB meeting.
28. Work with Change Manager to facilitate emergency changes.
29. Determine approvals and communicate with stakeholders for Emergency Changes.
30. Monitor execution of back-out plan when warranted.

Engage the Change Manager as necessary.

1. Train staff in principles, processes and procedures
2. Support OIT staff and stakeholders by providing process documentation, and conducting training in their areas of expertise.
3. Provide feedback and recommendations on the process and/or tools where needed.
4. Provide management information about change management quality and operations
5. Report violations and non-compliance to COR and VA PM(s) as required.

Deliverable:

1. Change Management Monthly report:
2. Forward Schedule of Change report

### RELEASE MANAGEMENT SUPPORT

The Contractor shall provide release management support at the ITIL program office level and support the ITIL functions of release management and build management, as they are executed throughout OIT. The ITIL release management discipline ensures that all components of product releases are organized and deployed in a controlled manner enabling a repeatable process. The Contractor shall review, analyze and standardize release and deployment processes and audit those processes as well. The Contractor shall support the design and implementation of formal procedures, including checks and balances throughout the process. The Contractor shall identify and mitigate risk to ensure the integrity and recoverability of the production environment and ensure the currency, accuracy, and completeness of the CMDB for all business and technical data elements for ITOPS applications.

The Contractor shall:

1. Comply with OIT Release Management policies and procedures.
2. Communicate and promote the process and initiate process improvements.
3. Plan and coordinate process training.
4. Be accountable for the overall effectiveness of the process.
5. Lead development and improvement effort for process engineering.
6. Promote release management awareness and understanding within the organization.
7. Manage all aspects of the end-to-end release and deployment process.
8. Ensure coordination of packaging, test and release teams.
9. Act as a liaison to appropriate management.
10. Form a release team to manage the many required activities by selecting team members, obtaining management approval, and assigning team roles and responsibilities.
11. Develop detailed release plans.
12. Facilitate team communication to ensure that releases are implemented according to schedule with system integrity and availability maintained.
13. Audit applications software and supporting hardware before and after the implementation of release package changes.
14. Plan the release and verify that all pieces of the Package Plan Checklist, Testing Checklist, Operations Readiness, and Rollout Checklist have been completed.
15. Coordinate with the appropriate parties, Operations Teams, Application Development Team and Testing Team to ensure the release is successfully planned for, tested and deployed.
16. Define the release and the release approach.
17. Create test plan, test use cases, and test scripts.
18. Perform functional, operational, performance, and integration testing.
19. Perform user acceptance testing (UAT) of approved changes.
20. Verify if expected results were achieved.
21. Train staff in release management principles, processes and procedures.
22. Provide management information about release management, quality, and operations.
23. Comply with VA and ITOPS IO security and privacy policies and directives, and CRISP. The Contractor shall take immediate action and ensure resolution of violations and non-compliance in regards to ITOPS IO and VA policies, procedures, directives, and management handbooks.
24. Report violations and non-compliance to COR and VA PM(s) as required.

###  ASSET MANAGEMENT AND LOGISTICAL SUPPORT

The Contractor shall provide asset management support to include, inventory and utilization of software and hardware assets.

The Contractor shall:

1. Ensure accurate inventory tracking data are promptly documented in the asset management tool Automated Engineering Management System/Medical Equipment Room Reporting (AEMS/MERS) or applicable asset management tool.
2. Perform Asset Management to include Asset Inventory/Audit & Tracking Asset Administration & Reporting, Integrated IT Asset Portfolio, and History and Forecasting, automating the asset management process as necessary.
3. Ensure accurate inventory tracking data are promptly reported in the asset management tool.

### DATABASE ADMINISTRATION SUPPORT

The Contractor shall provide services related to all types of data management, Database Management Systems (DBMS), and database applications including, but not limited to, logical and physical modeling and design/redesign, installation, administration, tailoring, tuning, troubleshooting, integrating, patching, upgrading, reporting, COOP, and backup/recovery/archiving/encryption and encryption key management. The Contractor shall develop, maintain, optimize, transition and decommission Extract Transform Load (ETL) capabilities and scripts de-personalization of data, and data protection procedure development. The Contractor shall also provide data mining and Business Intelligence (BI) expertise to include product recommendation, selection, implementation, dashboard and report development, BI strategies, decision support, and data/report distribution. The Contractor shall also provide expertise to include enterprise capture, curation, storage, search, processing, sharing, transfer, analysis, virtualization, etc. This expertise includes near real-time analytics including unstructured and structured, large and complex data on an enterprise scale. The Contractor shall meet broad-based interoperability requirements at the Federal, state and local level.

### SYSTEMS ARCHITECTURE SUPPORT

The Contractor shall provide analytical processes to the planning, design and implementation of new and improved information systems to meet the business requirements of customer organizations.

The Contractor shall:

1. Provide expert-level technical analysis, to include:
	1. Perform Gap analyses to define opportunities for new or improved business process solutions. Provide results to COR or assigned VA PM.
	2. Conduct business process engineering.
	3. Gather, describe, and document functional and system requirements using processes and methods in a broad range of IT activities and in-depth analysis of IT issues as necessary.
	4. Assist in refining system architecture objectives.
	5. Conduct feasibility studies and trade-off analyses. Analysis must be completed in the context of local, national and federal architectural standards. Deliver studies to COR or assigned VA PM.
2. Prepare business cases for the application of IT solutions.
3. Ensure the integration of all systems components, e.g., procedures, databases, policies, software, and hardware; planning systems implementation.
4. Ensure the rigorous application of information security/information assurance policies, principles, and practices to the systems analysis process.
5. Participate as a systems architect on various ITOPS projects.
6. Meet with customers, VA technical staff and management through in-person and remote settings.
7. Present information formally and informally, including business cases, systems designs, technology briefings and training to a variety of audiences.
8. Keep System Architecture documents up to date by utilizing ITOPS IO currently installed version of Microsoft Word, Excel, Visio, PowerPoint, SharePoint and other ITOPS IO currently supported tools to document deliverables, as necessary. Documents shall include specific configuration instructions, specifications, hardware and software requirements, implementation plans, version description, interface requirements/guide, administrative support guide, troubleshooting guides, user/analyst guide and physical and logical layer diagrams as necessary.
9. Use the standard ITOPS change management system to obtain new work assignments, update status and store work products as necessary.

**Deliverable:**

1. Gap analyses
2. Feasibility studies
3. Trade-off analyses

### ARCHITECTURE ASSESSMENT SUPPORT

This Contractor shall apply analytical processes to the planning, design and implementation of new and improved architectures and workflows to meet the business continuity requirements of customer organizations.

The Contractor shall:

1. Provide SME support for architectural design reviews and analyses including but not limited to Storage, Networks, Virtualization, and Backup.
2. Analyze technically agnostic independent best practices, and identify and make recommendations on architecture gaps related to staffing, training, process and workflows, and CM. Any recommendations shall be provided to the COR and VA PM(s) for approval prior to any implementation or changes.
3. Analyze Operational Risks and Assumptions.
4. Conduct feasibility and trade-off analyses. Analyses must be completed in the context of local, national and Federal architectural standards.
5. Ensure the integration of all systems components, e.g., procedures, databases, policies, software, and hardware; planning systems implementation.
6. Ensure the rigorous application of information security/information assurance policies, principles, and practices to the systems analysis process.
7. Function as a SME level systems analyst/solution architect on various ITOPS IO projects.
8. Facilitate in-person and remote customer meetings for VA technical staff and management.

### SYSTEMS ENGINEERING SUPPORT

The Contractor shall provide engineering expertise for planning, design and implementation of new and improved information systems. The Contractor shall provide analytical processes to meet the business requirements of customer organizations across ITOPS. The Contractor shall provide engineering support for requirements gathering, requirements management, use-case development, risk management, architecture design, performance engineering, capacity planning, system development, test and evaluation, and sustainment. The Contractor shall conduct trade-off/best technical approach analyses, analysis of alternatives, and engineering studies. The Contractor shall develop System Engineering Plans (SEPs), design plans, and technical reports as required. System software engineering support includes, but is not limited to, software system reliability assessments, and participation in Integrated Project Teams (IPT). The Contractor shall ensure the dependencies, interoperability, availability, reliability, maintainability and performance of the assigned systems.

The Contractor shall:

1. Provide services for evaluation, planning, requirements analysis, design, coding and unit testing, system integration testing, implementation, deploying, maintaining or updating a system.
2. Provide systems/software integration support to include planning, updating architecture models, interoperability specifications and analysis, system interface specifications, service definitions, and segmented architecture for the transition, integration, and implementation of IT systems.
3. Prepare, revise, or update engineering, user and technical documentation, reports, and manuals for projects, software applications or systems.
4. Perform gap analyses to define opportunities for new or improved system engineering solutions. Provide results to COR or assigned VA PM.
5. Gather, describe and document functional and system requirements using processes and methods in a broad range of IT activities and in-depth analysis of IT issues as necessary.
6. Refine system engineering objectives.
7. Develop cost estimates for new and modified systems, identify risks and assumptions, and provide results to COR or assigned VA PM.
8. Conduct feasibility studies and trade-off analyses. Analyses shall be completed in the context of local, national and Federal architectural standards. Deliver studies and analyses results to COR or assigned VA PM.

**Deliverable:**

1. System Engineering Plan

### **DESKTOP AND DEVICE ENGINEERING (DDE) SERVICES**

The Contractor shall provide engineering support at the ITOPS lab facility in Albany, NY, and remote services for the following work:

1. Application repackaging.
2. Application repackaging testing.
3. Request intake and management.
4. SharePoint site management.
5. Operating System Deployment (OSD) driver testing for hardware.
6. New and updated baseline development and testing.
7. Patching for OS and 3rd party.
8. Lab management activities.
9. OSD development and testing.
10. General lab activities.
11. Internal developed tool support.
12. CM engineering support for DDE activities.

### NETWORK AND TELECOMMUNICATION SUPPORT

The Contractor shall provide Tier 2 network infrastructure and telecommunications support (voice, voice over IP, and video) to its user base by providing data and voice connectivity support services. The Contractor shall provide mobile device issuance, administration, and support. The Contractor shall provide infrastructure installation support to its user base by supporting structured cabling and equipment deployment requirements. The Contractor shall provide enterprise connectivity support services in accordance with established ITOPS procedures and guidelines. The Contractor shall ensure that all enterprise connectivity support tasks are performed in accordance with applicable security regulations. Materials, hardware and software for network infrastructure and telecommunications installations will be furnished by the Government for installation by the Contractor as needed.

The Contractor shall:

1. Configure computer room cabinets for network and telecommunications hardware, and install hardware, software, cables, and power supplies.
2. Install infrastructure devices, network and telecom, which includes: configuration of assembly, cabling, power connection, cable routing and management, up to the Tier 3 configuration level. Contractor support shall include interfacing with Tier 3 VA Officials and Contractors for completion of device baseline configuration.
3. Initial triage of infrastructure (network switches and routers, and telecommunication devices). After triage, if the issue cannot be resolved at this level, the Contractor shall enter a Service Now incident request and assign to the appropriate Tier 3 group.
4. Provide infrastructure refresh installation services for bulk equipment deliveries at VA premises.
5. Provide infrastructure installation for activations of new VA premises.
6. Identify, triage, and resolve network and telecommunications customer issues and provide status to the customer within 72 hours.
7. Provide services for moves, adds, and changes on all systems required to issue, maintain, and service the network infrastructure telephony and mobile devices.
8. As part of the Contractor Progress and Monthly Status Report, provide a section to include status of service desk tickets processed. In this section, the Contractor shall highlight specific areas that may have been affected and provide an overview of the tickets the Contractor has worked in the network and telephone connectivity categories, for statistical purposes. The Contractor shall include information in this section to measure performance on production associated with data center network and telecommunications infrastructure, systems, and mobile devices.
9. Document procedures for all network infrastructure and telecommunications requirements in accordance with established ITOPS and/or VA guidelines and regulations.
10. Input inventory tracking data in asset management tools.
11. Provide a monthly status of on-going projects to the ITOPS VA PM and COR summarizing major activities performed during the month, identifying any issues or concerns.
12. Update in Service Now, the ITOPS ticketing tool, the status of requests, incidents, and change orders for each action to indicate work accomplished for specific requests.
13. Resolve customer support requests and incidents in ITOPS specified timeframes.
14. Ensure accurate inventory tracking data are promptly reported in the asset management tool.
15. Identify and report to the ITOPS PM all potential problems with processes, schedules, user requirements, that impact daily operations within the ITOPS relating to issues with enterprise connectivity.
16. Research to confirm information is accurate, and create documentation for subnets, IP ranges, VLANs, ACLs, and DHCP processes.

### APPLICATION MANAGEMENT SERVICES

The Contractor shall:

1. Provide application management subject matter expertise for one or more applications in the sustainment lifecycle. The Contractor shall monitor and measure application and infrastructure performance.
2. Serve as the SME for assigned applications, possessing a working knowledge of the application (including navigation and functionality) infrastructure, and security architecture.
3. Ensure all components of product releases, and infrastructure changes, are organized and deployed in a controlled manner enabling a repeatable process. Manage the release and deployment process. The Contractors release management support activities shall include design and implementation of formal procedures, including checks and balances throughout the process. The Contractor shall identify and mitigate risks to ensure the integrity and recoverability of the production environment. The Contractor shall ensure the currency, accuracy, and completeness of the CMDB for all business and technical data elements for assigned applications.
4. Ensure the currency, accuracy, and completeness of the CMDB, work management and mail group memberships, costs for assigned applications and projects, ATO and security artifacts, and security patches maintained.
5. Enforce compliance with VA security and privacy policies and directives, and the CRISP initiative. The Contractor shall take immediate action and ensure resolution of violations and non-compliance, ITOPS policies, procedures, directives, and management handbooks, and ITOPS and VA approved data storage backup policy.
6. Monitor and analyze application performance, capacity, reliability, and stability metrics. The Contractor shall take immediate corrective action to mitigate unacceptable performance levels, and develop plans for resolution.
7. Proactively manage server certificates. The Contractor shall maintain and publish a plan that identifies and tracks tasks, schedule, and ownership.
8. Manage application outage and Swift Action Response Team (SWAT) events, and proactively engage in root cause analyses.
9. Analyze and manage the Automated Notification Response (ANR) process, ensuring accuracy and completeness.
10. Conduct root cause analyses of application outages and create effective remediation plans.
11. Participate in the ITOPS Operations Planning meetings, assessing change impact, performing risk mitigation, and organizing communication plans. The Contractor shall serve as the primary technical SME point-of-contact for assigned applications, facilitating and coordinating customer requirements, integration efforts, and other actions, as required.
12. Provide SME recommendations to ITOPS during meetings, release management/operational readiness reviews, and other work sessions, such as planning and budgeting.
13. Participate in a matrix team environment, actively and effectively managing relationships with customers, build and release managers, technical teams, product development, project managers, and other stakeholders as required.
14. Ensure the currency, accuracy, completeness, and timely close-out of change orders, service requests, and incident reports, verification of all data storage back-ups for assigned applications, accuracy of all labor hours recorded in Primavera for assigned projects, and accurate and timely completion of server worksheets, storage request forms, firewall spreadsheets, and other artifacts required by internal ITOPS teams.
15. Maintain recorded labor hours associated with change orders, service requests, incident reports, and activity codes that accurately reflect the work performed for assigned applications. The Contractor shall take immediate corrective action when labor hours are not accurate, reporting discrepancies to the onsite Contractor Manager for contract resources, and including the Program Manager Serve as SME for internal-facing changes and activities, such as CRISP patching, load balancer upgrades, server builds and modifications, storage allocations, firewall changes, and other related activities.
16. Plan for systems implementation and continual improvement by participating in process design and implementation of procedures for the installation of changes to IT systems and infrastructure.
17. Keep the hardware inventory and software versions tracked and recorded in the CMDB.
18. Keep the CMDB current, accurate, and complete for assigned applications.
19. Conduct monthly audits of the CMDB and take immediate corrective action as required when deviations or missing data is found. The Contractor shall provide monthly documentation to the Program Manager on findings and actions.
20. Plan and manage changes and other deployment activities for assigned applications following release, configuration, and project management requirements, and applying ITIL processes according to ITOPS policies and procedures.
21. Ensure product releases for operational readiness while providing SME recommendation for the go/no go decision. The Contractor shall ensure that an approved plan is in-place with assigned ownership and schedule to resolve non-compliance issues.
22. Provide planning, coordination, and communication ensuring the successful deployment of software and infrastructure changes.
23. Ensure that only approved and tested product versions are installed in accordance with the ITOPS approved Process Management website.
24. Verify the accuracy and reliability of product release back out instructions.
25. Communicate the impact of planned releases to all stakeholders.
26. Assist in troubleshooting problems associated with a release.
27. Ensure compliance with ITOPS approved backup policy. The Contractor shall take immediate corrective action when compliance requirements are not met.
28. Monitor the VA TRM and develop compliance plans.
29. Proactively ensure that the Knowledge Management database contains accurate and current lessons learned and “how to” information.
30. Ensure that Risk Based Decision (RBD) memos are created according to directives, and are renewed prior to scheduled expiration. All work products shall be provided to COR and VA PM(s) for review prior to any distribution.
31. Ensure that POAMs are resolved and responded to as required.
32. Comply with VA security and Information Security policies and directives, and the CRISP. The Contractor shall take immediate action and ensure resolution of violations and non-compliance. The Contractor shall ensure compliance with ITOPS IO and VA policies, procedures, directives, and management handbooks.
33. Support approval of application access requests. The Contractor shall conduct access reviews in compliance with VA policy, including the closing of expired accounts.
34. Provide monthly status and action plans for outages, root cause analyses, remediation plans, risks and issues (in advance of a crisis), customer satisfaction, lifecycle plans, application metrics, trends, actions, and CRISP compliance.
35. Serve as backup to the application, build, or project manager, and other IT specialists.
36. Support and management of ITOPS service requests and development/oversight of service catalog items.

### APPLICATION ADMINISTRATION SUPPORT

The Contractor shall provide application administration support services for software in use by ITOPS.

The Contractor shall:

1. Install, sustain, and administer the application from an enterprise level.
2. Provide SME level knowledge to support the application including configuring and customizing the existing solution application.
3. Provide assistance to set up and maintain user accounts, assist with other software applications interfacing with existing applications, compile reports, respond to customer requests.
4. Monitor open tickets to ensure correct categorization and adhere to business processes.
5. Identify and report discrepancies along with proposed corrective action. Any action plans shall be provided to the COR/VA PM(s) prior to any implementation or changes.
6. Maintain knowledge based documents.
7. Evaluate application configuration and provide recommendations for improvement. Any recommendations shall be provided to the COR and VA PM(s) prior to any implementation or changes.
8. Provide industry and best practice technical recommendations and solutions within the ITIL framework. Any recommendations shall be provided to the COR and VA PM(s) prior to any implementation or changes.
9. Provide administration support by setting up notifications, service level agreements, access types, surveys, service contracts, and other application components.
10. Track and document all system changes, problems, issues, and workflow tasks according to VA policy through change orders, service requests, incident and/or problem tickets.
11. Participate and contribute at project meetings as SME for application administration related areas.
12. Support third party software application installs and configuration.
13. Assist users, software vendors, and other administrators (i.e.: database, network, systems, backup, and storage administrators) with problems, projects, and implementations of applications.
14. Install and implement new releases, functionality, and patches to applications.

### DESKTOP SUPPORT SERVICES

The Contractor shall provide desktop support services to ITOPS supported locations. This Contractor support shall also include wireless devices, to include iPhones and iPads, tablets, printers, and scanners, in support of ITOPS Microsoft Windows and client based environments, during normal hours of operation. The Contractor shall also provide first level support for telecommunication and video telecommunications devices. The Contractor shall ensure all workstations (the term workstation in this document means either a desktop or docked laptop) are configured to the most current VA approved OS. In addition, the Contractor shall augment the VA desktop support team to provide desktop support services in a Microsoft client/server environment. The Contractor shall perform desktop support services in accordance with established ITOPS procedures and guidelines. The Contractor shall ensure that all OS migrations and other desktop support tasks are performed in accordance with applicable security regulations and processes.

The Contractor shall:

* 1. Adhere to and assist in refining existing or new migration procedures to ensure that all user capabilities are transferred from the existing desktop or laptop computer to the new configuration. All recommended procedures shall be provided to COR and VA PM(s) prior to any migration.
	2. Provide methods and plans to support application and system OS upgrades and maintenance.
	3. Coordinate directly with users and/or their supervisors to minimize disruption of daily operations.
	4. Plan, deploy, manage and optimize Microsoft-based enterprise solutions.
	5. Identify and report to the COR and VA PM(s) all potential process, schedule, or user requirement problems that may adversely affect daily operations.
	6. Provide Desktop security support using ITOPS established security procedures for desktops, which may necessitate assisting in developing new security plans.
	7. Utilize Microsoft System Center Operations Manager (SCOM) and SCOM tools to troubleshoot performance issues and deploy software packages, to include Scripting, McAfee and other VA standard tools.
	8. Install and implement new releases and patches to the OS software and standard applications when approved by VA.
	9. Implement security hardening requirements and structures provided by security division to secure the operating system structures to prevent unauthorized access and denied access to systems.
	10. Create and maintain local documentation related to Window system administration installation and configuration guides, as well as procedures and policies.
	11. Perform asset management to include asset inventory, audit and tracking, asset administration and reporting, integrated IT asset portfolio, and history and forecasting, automating the asset management process as necessary.
	12. Ensure accurate inventory tracking data is promptly reported in the asset management tool.
	13. Track and document all system changes, problems, issues, and work tasks within Service Now, the ITOPS service desk tool.
	14. Update service requests no fewer than every three (3) business days, and update change-orders every five (5) business days for each action to indicate work accomplished for specific service requests or change orders.
	15. Submit change-orders five (5) days prior to work being performed.
	16. Respond within 2 hours of notification that a problem has occurred.
	17. Perform software application installation and configuration based on change order instructions. The Contractor shall follow established ITOPS change order processes.
	18. Provide first line support for Video Teleconference (VTC) requests or related issues when required.
	19. Within the Contractor’s Progress, Status, and Management Report, the Contractor shall include a section which includes the following:
	20. Compliance Report to measure the number of desktops and laptops up to date with respect to the following: Encryption software, Microsoft security patches, McAfee McAfee ePolicy Orchestrator (EPO).
	21. Support Requests Report to measure number of support requests closed in the past 24, 48, 72, 120 and greater than 120 hours.
	22. Status Report to summarize major activities performed during the month identifies any issues or concerns.
	23. Asset Management Report to summarize Asset Management Activity (Inventory of hardware and software)
	24. Support Remote customer through approved support tools and processes.

### DESKTOP PROVISIONING SUPPORT

The Contractor shall provide onsite desktop support and computer services for desktops, laptops, and peripheral devices, in support of ITOPS operational support requirements.

The Contractor shall:

1. Receive and unpack laptops/desktop computers upon receipt of shipment; configure new laptops/computers/hardware/software in accordance with ITOPS IO procedures, guidelines and applicable security regulations.
2. Test each laptop/computer to ensure its functionality meets established guidelines and regulations.
3. Issue the desktop computers and laptops to approved users and provide training on its use.
4. Resolve Customer support requests within five (5) business days. VA PM approval shall be required for any extension beyond five (5) business days, with exception of support requests associated with ordering, software, hardware and/or a service repair request, and Change Orders. The Contractor is not required to provide any software or hardware as part of this task.
5. Provide desktop installation services for activations on VA premises.
6. Provide desktop installation services for technology refresh delivered to VA premises.
7. Ensure accurate inventory tracking data are promptly documented in the asset management tool Automated Engineering Management System/Medical Equipment Room Reporting (AEMS/MERS) or applicable asset management tool.
8. Implement desktop provisioning standards, processes and security measures.
9. Comply with and support all Federal, VA, and ITOPS security regulations. and policies applicable to desktop provisioning support.
10. Update support requests, incidents, and change orders to indicate work accomplished.
11. Update provisioning service requests no less than every three (3) business days and change orders every five (5) business days for each action to indicate work accomplished for specific service requests or change orders.
12. Maintain the Hardware and Software Inventory and Configuration Log.
13. Prepare Change Orders.
14. Support remote customers only through approved support tools and processes.
15. Perform media sanitization, disposal and/or turn in of equipment.

### CONTINUITY OF OPERATIONS (COOP) SUPPORT

The Contractor shall complete a thorough review and analysis of all past and present Information System Contingency Plans (ISCP) and other audits, i.e. Security audits (OIG and SCA).

The Contractor shall create the following Disaster recovery plans:

1. Required Plans

a. General System Support (GSS) Information System Contingency Plan (ISCP)

b. Enterprise Data Hosting Center(s) Disaster Recovery Plan

c. Shared Infrastructure System Contingency Plan (ISCP)

d. VistA Information System Contingency Plan

e. EUO Site IS Outage Escalation Plan and any additional site-specific plans

1. Document and aid with testing all COOP plans to include ISCP and disaster recovery plans.
2. Provide recommendations, after reviewing white papers and/or other documents pertaining to the disaster recovery COOP processes and procedures. All documentation created as a result of these services shall be provided to the COR.

**Deliverables:**

1. Disaster Recovery Plans
2. VA Enterprise Test and Information System Contingency Plans (ISCP)

## Transition Plan (Optional Task)

If required, the Contractor shall develop, document, and monitor the execution of a transition plan that may be used to transition to a new Contractor or to the Government. The Contractor shall provide an oral presentation which shall be scheduled in coordination with the COR, and its transition plan shall include written supporting documentation (technical, procedural, or policy-based) that summarizes the delivery of services as required by this TO. All final reports, status updates, and transfer of all appropriate records (including electronic information) to the COR shall be accomplished at the completion of this TO. Transition activities shall be performed onsite at each location as necessary.

Deliverable:

A. Transition Plan

# GENERAL REQUIREMENTS

## PERFORMANCE METRICS

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

| **Performance Objective** | **Performance Standard** | **Acceptable Levels of Performance** |
| --- | --- | --- |
| 1. Technical / Quality of Product or Service
 | 1. Shows understanding of requirements
2. Efficient and effective in meeting requirements
3. Meets technical needs and mission requirements
4. Provides quality services/products
 | Satisfactory or higher |
| 1. Project Milestones and Schedule
 | 1. Quick response capability
2. Products completed, reviewed, delivered in accordance with the established schedule
3. Notifies customer in advance of potential problems
 | Satisfactory or higher |
| 1. Cost & Staffing
 | 1. Currency of expertise and staffing levels appropriate
2. Personnel possess necessary knowledge, skills and abilities to perform tasks
 | Satisfactory or higher |
| 1. Management
 | 1. Integration and coordination of all activities to execute effort
 | Satisfactory or higher |

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the TO 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 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.

## SECTION 508 – ELECTRONIC AND INFORMATION TECHNOLOGY (EIT) STANDARDS

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 are 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.

The following Section 508 Requirements supersede Addendum A, Section A3 from the T4NG Basic PWS.

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>. A printed copy of the standards will be supplied upon request.  The Contractor shall comply with the technical standards as marked:

[x]  § 1194.21 Software applications and operating systems

[x]  § 1194.22 Web-based intranet and internet information and applications

[x]  § 1194.23 Telecommunications products

[x]  § 1194.24 Video and multimedia products

[x]  § 1194.25 Self-contained, closed products

[x]  § 1194.26 Desktop and portable computers

[x]  § 1194.31 Functional Performance Criteria

[x]  § 1194.41 Information, Documentation, and Support

### 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.

### 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.

### 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.

**Deliverable:**

* + - 1. Final Section 508 Compliance Test Results
	1. **SEGREGATION OF DUTIES**

VA is concerned that a segregation of duties conflict may arise during the period of performance of this order and any tasks required. A segregation of duties conflict may arise if an entity manages and/or develops a system and then assesses the security posture of that system. As a safeguard against this conflict, the Contractor agrees to notify the CO within 24 hours, or the next working day, if it discovers that the Contractor, or one of its subcontractors, is auditing a VA system that the Contractor or subcontractor developed or managed, assisted with the development or management of, or provided other such services that may lead to a segregation of duties conflict. VA will then conduct an independent assessment of the Contractor’s work to ensure transparency and accuracy. The Contractor shall provide a mitigation plan to the CO. At a minimum, the mitigation plan shall include:

1. List of any systems developed or managed by the Contractor for VA;
2. Procedures to prevent the auditors from learning which VA systems are included in the IP range being audited;
3. Procedures to prevent the unauthorized disclosure or improper use of sensitive or proprietary information that the auditors may obtain; and
4. The establishment of employee training programs to ensure complete awareness and effective implementation of all aspects of the mitigation plan.

## ORGANIZATIONAL CONFLICT of INTEREST

Please be advised that since the awardee of this Task Order will provide remediation and IT support services, some restrictions on future activities of the awardee may be required in accordance with FAR 9.5 and the clause entitled, Organizational Conflict of Interest, found in Section H of the T4NG basic contract. The Contractor and its employees, as appropriate, shall be required to sign Non-Disclosure Agreements (Appendix A).

# APPENDIX A

CONTRACTOR NON-DISCLOSURE AGREEMENT

This Agreement refers to Contract/Order \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ entered into between the Department of Veterans Affairs and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Contractor).

**As an officer of** <fill in name of Contractor>**, authorized to bind the company, I understand that in connection with our participation in the** <fill in program> **acquisition under the subject Contract/Order, Contractor’s employees may acquire or have access to procurement sensitive or source selection information relating to any aspect of** <fill in program> **acquisition. Company**<fill in name> **hereby agrees that it will obtain Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements from any and all employees who will be tasked to perform work under the subject Contract/Order prior to their assignment to that Contract/Order. The Company shall provide a copy of each signed agreement to the Contracting Officer. Company** <fill in name> **acknowledges that the Contractor - Employee Personal Financial Interest/Protection of Sensitive Information Agreements require Contractor’s employee(s) to promptly notify Company management in the event that the employee releases any of the information covered by that agreement and/or whether during the course of their participation, the employee, his or her spouse, minor children or any member of the employee’s immediate family/household has/or acquires any holdings or interest whatsoever in any other private organization (e.g., contractors, offerors, their subcontractors, joint venture partners, or team members), identified to the employee during the course of the employee’s participation, which may have an interest in the matter the Company is supporting pursuant to the above stated Contract/Order. The Company agrees to educate its employees in regard to their conflict of interest responsibilities.**

Company <fill in name>further agrees that it will notify the Contracting Officer within 24 hours, or the next working day, whichever is later, of any employee violation. The notification will identify the business organization or other entity, or individual person, to whom the information in question was divulged and the content of that information. Company <fill in name>agrees, in the event of such notification, that, unless authorized otherwise by the Contracting Officer, it will immediately withdraw that employee from further participation in the acquisition until the Organizational Conflict of Interest issue is resolved.

This agreement shall be interpreted under and in conformance with the laws of the United States.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature and Date Company

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name Phone Number

CONTRACTOR EMPLOYEE

PERSONAL FINANCIAL INTEREST/PROTECTION OF SENSITIVE INFORMATION AGREEMENT

This Agreement refers to Contract/Order \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ entered into between the Department of Veterans Affairs and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Contractor).

As an employee of the aforementioned Contractor, I understand that in connection with my involvement in the support of the above-referenced Contract/Order, I may receive or have access to certain “sensitive information” relating to said Contract/Order, and/or may be called upon to perform services which could have a potential impact on the financial interests of other companies, businesses or corporate entities. I hereby agree that I will not discuss or otherwise disclose (except as may be legally or contractually required) any such “sensitive information” maintained by the Department of Veterans Affairs or by others on behalf of the Department of Veterans Affairs, to any person, including personnel in my own organization, not authorized to receive such information.

“Sensitive information” includes:

1. Information provided to the Contractor or the Government that would be competitively useful on current or future related procurements; or
2. Is considered source selection information or bid and proposal information as defined in FAR 2.101, and FAR 3.104-4; or
3. Contains (1) information about a Contractor’s pricing, rates, costs, schedule, or contract performance; or (2) the Government’s analysis of that information; or
4. Program information relating to current or estimated budgets, schedules or other financial information relating to the program office; or

(e) Is properly marked as source selection information or any similar markings.

Should “sensitive information” be provided to me under this Contract/Order, I agree not to discuss or disclose such information with/to any individual not authorized to receive such information. If there is any uncertainty as to whether the disclosed information comprises “sensitive information”, I will request my employer to request a determination in writing from the Department of Veterans Affairs Contracting Officer as to the need to protect this information from disclosure.

I will promptly notify my employer if, during my participation in the subject Contract/Order, I am assigned any duties that could affect the interests of a company, business or corporate entity in which either I, my spouse or minor children, or any member of my immediate family/household has a personal financial interest. “Financial interest” is defined as compensation for employment in the form of wages, salaries, commissions, professional fees, or fees for business referrals, or any financial investments in the business in the form of direct stocks or bond ownership, or partnership interest (excluding non-directed retirement or other mutual fund investments). In the event that, at a later date, I acquire actual knowledge of such an interest or my employer becomes involved in proposing for a solicitation resulting from the work under this Contract/Order, as either an offeror, an advisor to an offeror, or as a Subcontractor to an offeror, I will promptly notify my employer. I understand this may disqualify me from any further involvement with this Contract/Order, as agreed upon between the Department of Veterans Affairs and my company.

Among the possible consequences, I understand that violation of any of the above conditions/requirements may result in my immediate disqualification or termination from working on this Contract/Order pending legal and contractual review.

I further understand and agree that all Confidential, Proprietary and/or Sensitive Information shall be retained, disseminated, released, and destroyed in accordance with the requirements of law and applicable Federal or Department of Veterans Affairs directives, regulations, instructions, policies and guidance.

This Agreement shall be interpreted under and in conformance with the laws of the United States.

I agree to the Terms of this Agreement and certify that I have read and understand the above Agreement. I further certify that the statements made herein are true and correct.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature and Date Company

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name Phone Number