Department of Defense
Defense Health Agency
DAD IO/J-6

Military Health System
Enterprise IT Services Integrator
(MHS EITSI)

Blanket Purchase Agreement (BPA)
Performance Work Statement (PWS)

Solicitation Number:

Version: 1.0

Date: 9/11/2020

PART 1
1.0 GENERAL INFORMATION

1.1 General Information

This is a single award, non-personal services Blanket Purchase Agreement (BPA) to provide Assistant Director Healthcare Administration, Deputy Assistant Director of Information Operations/J-6 (DAD IO/J-6) Military Health System Enterprise Information Technology Services Integrator (MHS EITSI) heretofore known as EITSI. This PWS broadly outlines the scope of the BPA; specific scope, tasks, funding, and deliverables will be defined in individual Call Order PWSs.

1.2 Introduction

The Defense Health Agency (DHA) was created as a joint, integrated Combat Support Agency (CSA) that supports the delivery of integrated, affordable, and quality health services to Military Health System (MHS) beneficiaries. It is responsible for driving integration of clinical and business processes across the MHS through a shared-service strategy.

The Department of Defense (DoD) began a multi-year transition of military Medical Treatment Facilities (MTFs) from the military service departments to DHA for purposes of implementing an integrated system of readiness and health as required by Section 702 of the National Defense Authorization Act (NDAA) for fiscal year (FY) 2017 and updated in the FY 2019 NDAA. At the end of the transition, all DoD MTFs will be subject to authority, direction, and control (ADC) of DHA through DHA's market-based management model. This ADC will include all Information Technology (IT) services and support capability, as well as transition to DHA of any existing and proposed operations support staff currently delivering those IT service and support capabilities under MTF control. The intention is to sustainably control and reduce operational costs by establishing rigorous control, accountability, traceability, and transparency with operational efficiencies gained through a large Enterprise shared-services model.

One of the directives given to the MHS was to deliver a single Electronic Health Record (EHR). The Defense Healthcare Management System Modernization (DHMSM) Program Management Office has the explicit mission to field this modernized EHR system, supporting an estimate 9 million beneficiaries and replacing MHS legacy systems to result in an intricate system of systems framework wholly dependent upon the underpinning and supporting data communications network and Enterprise services infrastructure, including data center(s), server hosting, and end-user platform capabilities.

In support of DHMSM, DHA is in the process of performing Enterprise infrastructure consolidation through the Desktop-to-Datacenter Program Executive Office (D2D PEO). D2D PEO enables the medical mission to be achieved through a platform that allows providers to access systems, move seamlessly and exchange health information and medical records across the Enterprise with trusted partners. Upon completion of all the components of D2D-PEO, the sites will benefit from increased standard technology services and business efficiencies. Currently, D2D-PEO is projected to be complete in FY21.

The DAD IO/J-6 is tasked to provide a standardized, robust, and highly available infrastructure and Enterprise-shared IT services through which DHMSM can achieve its EHR goal while adhering to the cost containment and operational efficiency standards driven by recent legislation (i.e., FY 2017 and FY 2019 NDAAs).

The DHA IT Enterprise supports 1,212 physical buildings (CONUS)/(OCONUS) of which nearly half are inpatient and smaller clinics and ancillary treatment facilities, with the remainder being administrative or educational research installations. These inpatient and smaller clinics, and ancillary treatment facilities are broken down as: 55 Military Medical Centers and Inpatient Hospitals, 373 Health Clinics, 245 Dental Clinics, and 5 Theater Hospitals.

The enterprise supports an estimated 850,000 network connected devices (i.e., end-user devices, servers, printers, network connection and protection). Total users are approximately 450,000 with 257,000 users at MTFs, and an estimated 205,000 of which are health care professionals and support staff. The DHA Global Service Center (GSC) handles approximately 78,000 calls per month, which are part of an estimated 90,000 incidents and requests processed per month.

The move to a single Enterprise strategy for IT support aligns with the August 15, 2019 Deputy Secretary of Defense Memorandum titled Fourth Estate Network Optimization (4ENO) Execution Guidance, where common use IT assets and services will be transferred to the Defense Information Systems Agency (DISA). The DHA is tentatively scheduled to move its service desk activities to DISA's Defense Enclave Service (DES) contract in FY25. DES is a collection of common use IT capabilities combined for efficient delivery and intends to provide a variety of IT services from the network transport layer to the desktop. It seeks to fill a wide range of IT requirements and deliver IT services to end-point devices at an affordable cost with superior performance. DISA and DHA plan to begin work to facilitate this move in FY23 to ensure a successful migration to DES in FY25.

1.3 Background

The DHA DAD/IO J-6 seeks to align enterprise IT services, standardize processes and procedures, and to reduce the large decentralized onsite touch labor presence, to provide more mature and centrally managed services and transition to more enterprise-wide services that support a federated customer base.

1.3.1 Strategy

DHA analyzed various potential strategies to provide the operational structures and required levels of governance and staff to provide effective sustainment and support across the entire DHA MHS operational landscape while adhering to NDAA mandates and alignment with DHA's overall IT strategy.

The selected strategy is to establish an Enterprise IT Services (EITS) Environment using a Multisourcing Services Integrator (MSI) approach. This strategy optimizes centralized control by awarding coordination, integration, and management activities to a contractor that specializes in these capabilities. It enables reduction of site-specific solutions and increases in centrally managed IT services because separate contracts, henceforth known as Service Providers (SPs), can be awarded for new or modernized services while the MSI provides

continuity. Throughout this document the MSI is referred to as the Enterprise Information Technology Services Integrator (EITSI).

1.3.2 Assumptions and Constraints

The following statements of assumptions and constraints are relevant to this BPA PWS:

- DHA will utilize Information Technology Service Management (ITSM) which covers incident management, problem management, change management, configuration management, knowledge management, service catalog management, and request management capabilities.
- DHA will use ServiceNow's ITSM suite of products to operate and support its infrastructure transition and sustainment according to industry best practices, to include: Information Technology Infrastructure Library (ITIL), Agile, Scrum, and Development and Operations (DevOps) based processes.
- DHA will provide an ITSM software solution and licenses for use to the EITSI and other service providers. DHA has acquired ServiceNow as its ITSM tool. Other tools are referenced in 5.2.7 Service Management Systems.
- DHA will leverage operational and industry best practices for service delivery and support, including Enterprise ITIL-based practices, such as problem management for recording, managing and eliminating recurrent or chronic failures, configuration baseline management and change control for recording and executing infrastructure changes identified as necessary to meet operational objectives; all while minimizing adverse risks to overall service availability and component and service capacity, demand management, and availability management.
- DHA expects to move to the ITIL 4 framework as part of establishing the EITS Environment, and thereby evolve from the current processes that conform to ITILv3 or do not follow ITIL practices at all.
- DHA will continue to deliver shared services equal to or better than existing capabilities and service expectations.
- All IT infrastructures will have a valid Life Cycle Management Plan (LCMP) in adherence to the corresponding Authority to Operate (ATO).
- Once D2D-PEO is complete, the Enterprise will be on a standardized transport via Multiprotocol Label Switching cloud network known as the Medical Community of Interest (Med-COI) and operating on the Medical Joint Active Directory (mJAD). Med-COI is the common network transport for MHS services. mJAD provides single common authentication and centralized identity management framework for the MHS.
- DHA will leverage DoD Enterprise Cloud Environment, a multi-cloud, multi-vendor ecosystem of cloud services. Traffic to and from these multi-cloud environments into Med-COI must ingress and egress through Med-COI Cloud Access Points (CAPs) for proper inspection. EITSI may need to work with existing Infrastructure & Operations Division's (IOD) Branches to migrate or assist MTFs, sites and geographically separated units (GSUs) with migration activities post D2D-PEO and MHS GENESIS Go Live.
- Operations will leverage standardized enterprise management tools, as selected by the DAD IO/J-6 Enterprise tools rationalization process.

- Tools such as Microsoft Systems Center Configuration Management (SCCM), System Center Operations Manager and Tanium will continue to be used to routinely inventory, centrally manage, and deliver digital content (patches, software, or updates) through distribution points and ensure all device end-points are visible by the Global Network Operations Center (GNOC). These Enterprise tools may change in the future.
- DHA will transition from DoD Enterprise E-mail to Defense Enterprise Office Solutions (DEOS) in Fiscal Year (FY) 21.
- Some DHA DAD IO/J-6 IT functions overlap between site and Enterprise levels.
- Local MTFs, clinics, and GSUs will have local compute capability that will eventually be incorporated into standardized Hosting and Cloud Support Services. Until that occurs, multiple local compute, storage, backup, and virtualization infrastructures will be supported and maintained in adherence to the ATOs.
- DHA Customers include Other Lines of Business (OLB) that are either associated with an MTF or provide additional supporting activities to the DHA mission.
- The DHA GSC and GNOC is projected to relocate to Port San Antonio in June 2021.
- DHA expects to begin work on the 4ENO Transition in 2023, and potentially moving in 2025.

1.3.3 Enterprise IT Services Environment

The EITS Environment is being established by DAD IO/J-6 as a multi-provider, integrated platform for the delivery of IT services to the DHA and MHS. This environment requires coordination, cooperation, communication, and integration among the EITSI, Service Providers, and Mission Partners with a goal of providing uninterrupted, high quality IT services to the DHA. The EITS Environment is the aggregation of IT delivery, management, and governance activities that allow for effective service delivery, timely decisions, and continuous improvement. See **Figure 1: Enterprise IT Services (EITS) Environment** below.

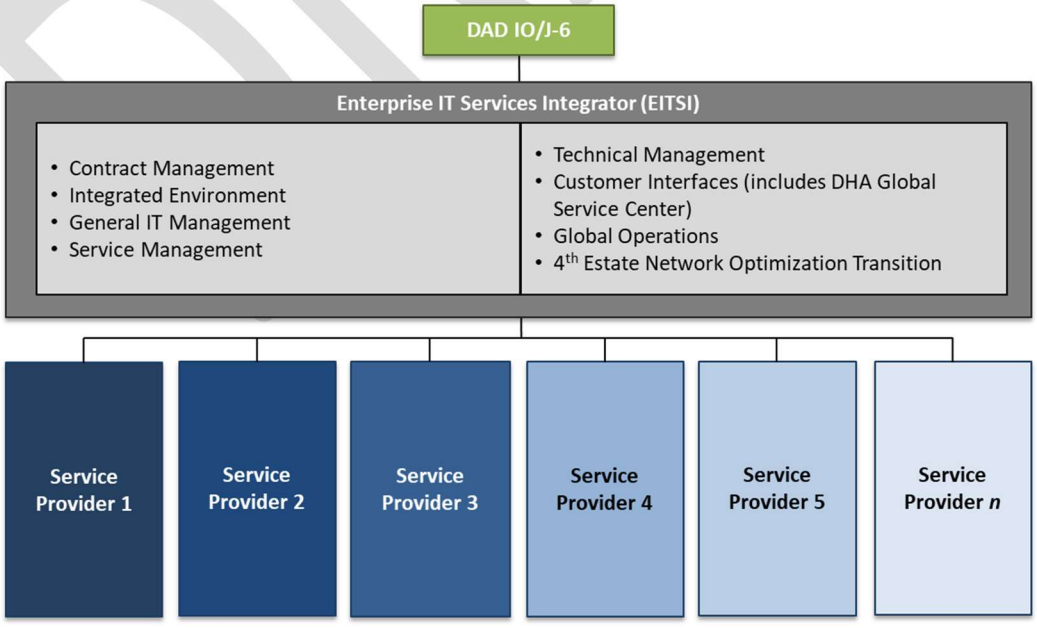

Figure 1: Enterprise IT Services (EITS) Environment

Key EITS Environment Features

Service Management Manual (SMM): The SMM will be the overarching operating procedures for the EITS Environment. It is the operational document repository that includes process descriptions, roles and responsibilities, policies, processes, and procedures.

Governance Model: Governance ensures Customer objectives are continually met through a healthy service provider relationship. It clarifies decision making and provides transparency through forums, clarified roles, and customer and Mission Partner engagement.

Service Level Agreements (SLAs): Service Levels communicate performance expectations to Customers, identify opportunities for improvement, and incentivize contractor performance. In a multisourced environment, contracts establish shared incentives for success.

Operating Level Agreements (OLAs): Formal agreements between two contractors that document the inter-dependencies for one or both to meet their obligations to the ultimate customer, in this case the DHA. OLAs include interaction rules between the parties, process flows, and handoff metrics.

DAD IO/J-6's role is management and oversight of the contractors performing in the EITS Environment. DAD IO/J-6 will establish and lead a governance framework with assistance from the EITSI that will include the forums, functions, and initiatives needed to facilitate involvement of the DHA, MHS, and Customers in day-to-day operations, service restorations, and issue resolution.

1.3.3.1 Enterprise IT Services Integrator

The EITSI role is defined by four main service elements listed below. The EITSI will bring these service elements together with stability and predictability to address changes in SPs, technology, and organizational demands while delivering consistently high levels of service to Customers.

- **Cross-functional**: professionalizing the cross-functional elements that enable successful delivery of cross-service provider and cross-capability services.
- **Coordination**: ensuring that service elements from multiple SPs, be they internal, unique, legacy, delivered by several similar providers or as a service from the cloud, come together to provide an acceptable business service to users.
- **Collaboration**: creating a platform of practice underpinned by agreement between the parties to ensure they all work together toward a common mission, because they see their own advantage in so doing.
- **Control**: operating on behalf of the MHS consistently and predictably.

The EITSI contractor will manage the EITS Environment and assist the Government in providing oversight of the SPs for the benefit of the DHA, MHS, and Mission Partners. The EITSI will provide independent end-to-end accountability through coordination and validation of IT services delivered by separately contracted SPs.

Goals for the EITSI model:

- Works toward the common goal of providing uninterrupted, secure, high quality services to the DHA, MHS, and Mission Partners.
- Ensures EITSI and SPs will perform their services, interact, and cooperate with each other within the EITS Environment in a manner that prioritizes the best interest of the DHA and its MHS customers.
- Supports relational and operational governance for the EITS Environment.
- Grounded in the ITIL 4 framework and focused on accountability, boundaries, and consistency while maturing delivery through continual improvements in the entire environment including cost effectiveness, service quality, value delivery, and customer experience.
- Supplants certain enterprise IT contracts supporting the DHA, MHS, and Mission Partners.
- Provides centralized reporting and management for the services within the EITS Environment while the EITSI acts as the single point of contact to the DHA, MHS, and Mission Partners.
- Provides oversight and coordination to the SPs on behalf of the DHA, including collaborating with SPs on services provided, issues, and issue resolutions.

The EITS Environment functions between the SPs performing day-to-day operational functions and the EITSI providing oversight and coordination as well as select service delivery functions such as the DHA Global Service Center (GSC) service desk. See **Figure 2: EITSI and Service Providers Roles** below.

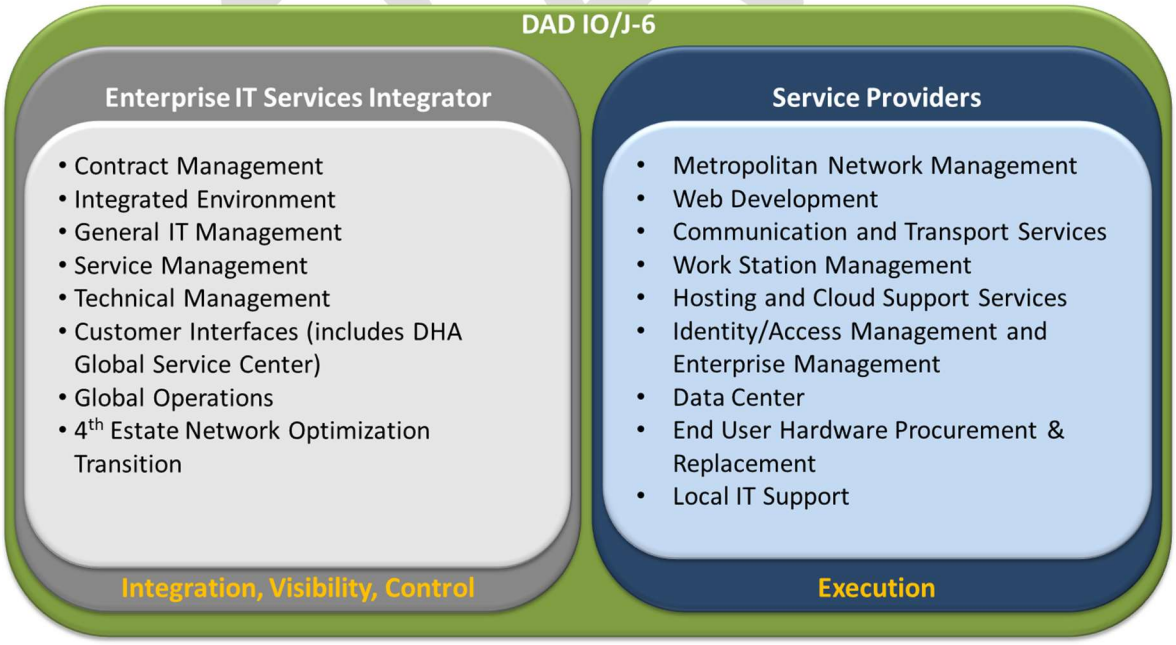

Figure 2: EITSI and Service Providers Roles

The specific scope areas and division of those scope areas for the Service Providers will be identified after award of the EITSI BPA. **Figure 2: EITSI and Service Providers Roles**

provides some examples. The Government expects some of the SPs to have an enterprise focus (i.e., the MHS enterprise) and some to have a more regional focus (e.g., Europe, Northwest CONUS, or smaller markets). At this time, those with an enterprise focus are referred to as Capability Service Providers (CSPs) and those with a regional focus are referred to as Geographic Service Providers (GSPs). Each of the SPs are expected to have a separate contract with the Government. The EITSI has specific Organizational Conflict of Interest (OCI) limitations on its ability to participate in these SP contracts.

This BPA PWS calls out Integrated Service Providers as all the SPs delivering services to Customers in the EITS Environment (i.e., EITSI, CSPs, GSPs, and Mission Partners identified by the Government).

The EITS Environment will ensure standardization through consistent policies, processes, tools, and reporting for all SPs. SPs will be modular and follow predefined sets of processes and tools aimed at quality of service and reducing costs. The EITSI will develop, coordinate, and maintain shared SLAs and OLAs to govern and incent cooperation between SPs aimed at increasing the quality of service to the DHA and its MHS customers. To ensure a successful transformation, the EITSI will pioneer DHA's IT transformation through innovation, organizational change management, and a formal governance structure. See **Figure 3: EITS Environment and Organization** below.

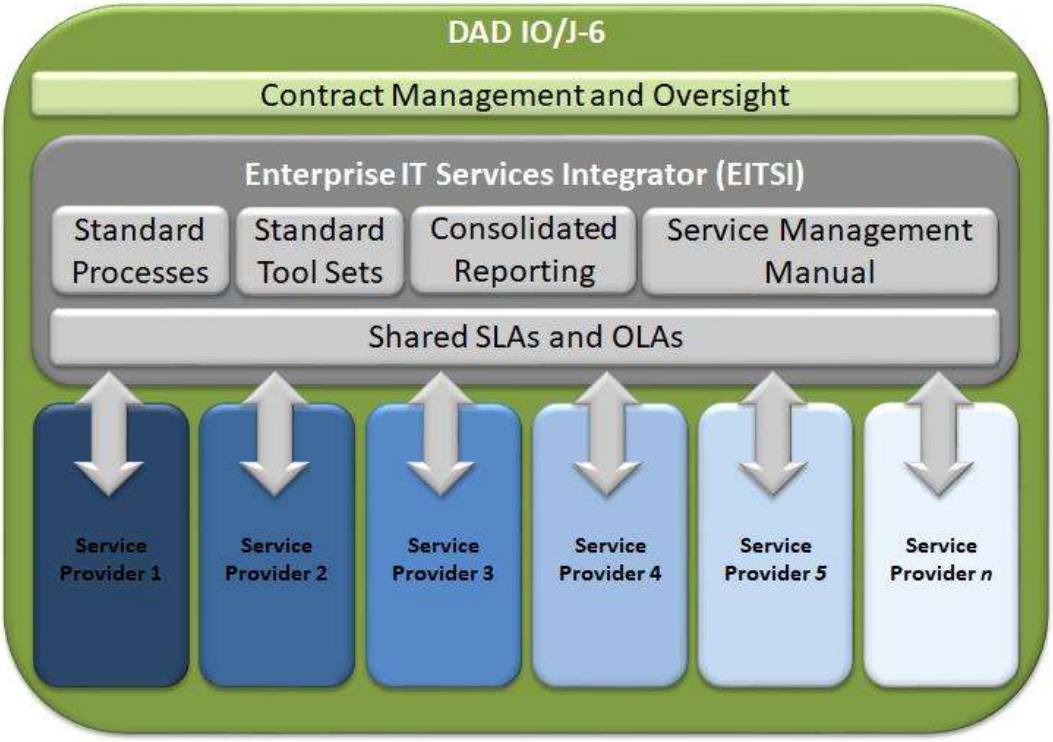

Figure 3: EITS Environment and Organization

1.3.3.2 EITS Governance Framework

The EITS Governance Framework strives to ensure DHA and MHS objectives are continually met. Utilizing various forums, communications, clarified roles, and continuous customer engagement the Governance Framework clarifies decision making and provides transparency to DAD IO/J-6, the MHS, EITSI, and Service Providers.

The governance framework will manage the contractual requirements and performance of service providers, maintain relationships with Customers, and monitor the ability of DHA and the Integrated Service Providers to meet the goals outlined in this PWS and any Call Orders placed against this BPA.

To accomplish this, the framework makes a distinction between Relational Governance and Operational Governance, and establishes a series of Relational and Operational Forums that are integral to the successful governance structure as shown in **Figure 4: EITS Governance Framework**

below. The forums provide for participants to understand each other's objectives, to ensure commitments are being met, and to implement changes as needed.

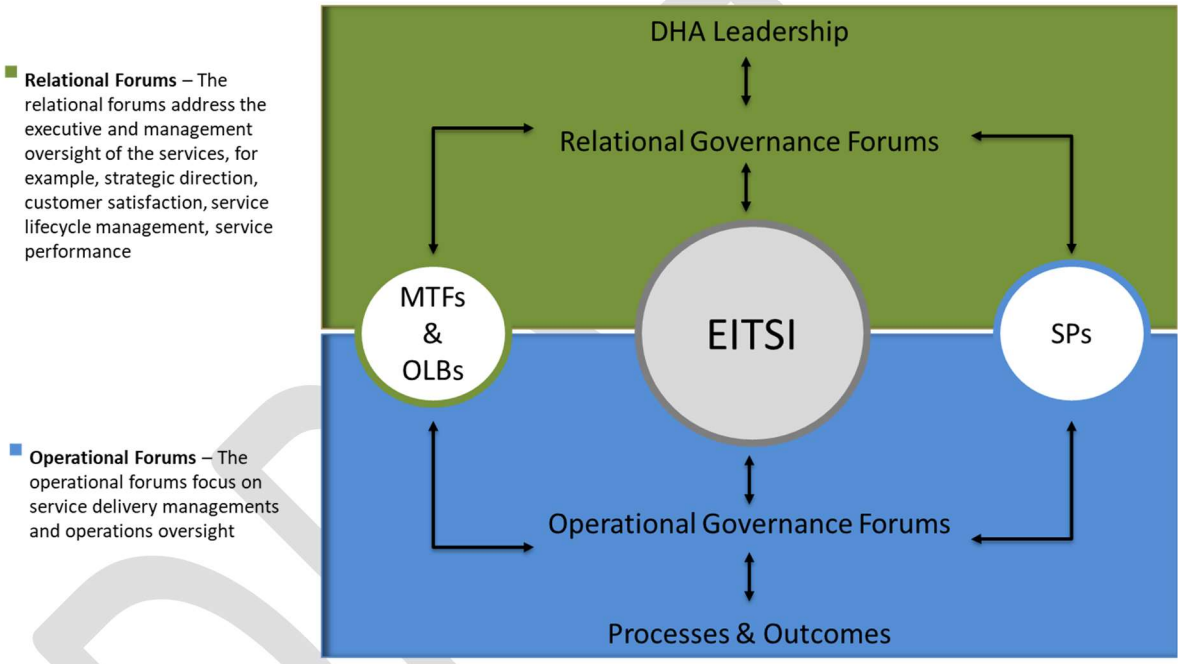

Figure 4: EITS Governance Framework

To ensure accountability and to preserve the decision rights, the DHA Leadership sits at the top of the EITS Governance framework. The Government will establish and lead the Relational Governance Forums, and participate with the EITSI in the Operational Governance forums. Because decision rights are retained by Government, the Relational Governance forums serve as the primary focal point for issue escalation and resolution. Relational Governance focuses on strategic issues, including the relationships among stakeholders, the ability of the EITS Environment to meet changing Customer needs, risk management, and support from the Enterprise for change.

The Operational Forums will be established and led by the EITSI and overseen by the Government; they will be grounded in ITIL 4 processes and align with the EITSI core functions. Operational components will be defined by the Customers together with SPs and are aligned with the processes as defined in the SMM. This includes processes such as issue resolution, service level management, change management, risk management, and reporting.

The Government expects the EITSI to manage Operational Forums, coordinate across forums, and drive the decisions made in those forums.

The Government anticipates that all Integrated Service Providers will collaborate with Government to establish and improve governance processes, particularly at the operational layer. This framework will continue to evolve as the parties identify opportunities to enhance the EITS Environment.

See Part 5 section 5.2.2 EITS Governance for requirements for the EITS Governance Framework.

1.4 Objectives

The EITSI will establish and manage an integrated environment for the delivery of IT services to the DHA and MHS. The overall objectives of the MHS EITS initiative are to:

- Deliver standardized sustainment processes
- Enable organizational agility to meet evolving mission demands
- Proactively drive innovation to directly increase operational efficiency
- Enable growth of common technical competencies between disparate support teams
- Create a method for sustained cost control through process standardization and work redefinition and redirection that reduces cost of performance

1.5 Scope

The Contractor shall provide everything under Scope as the Contractor Services. The Contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform tasks for MHS EITS as defined in this PWS and any Call Orders placed against this BPA that are issued except for those items specified as Government furnished property and services in **Part 3 Government Furnished Property, Equipment and Services**. The Contractor shall operate the EITS Environment which is an aggregation of IT delivery, management, and relationship activities that allow for effective service delivery, timely decisions, and continuous improvement. The Contractor shall perform to the standards in this PWS and Call Order PWSs.

1.6 Period of Performance

This is a potential 10-year BPA, comprised of a 1-year base period and nine 1-year option periods, targeted to be effective FY21 through FY31.

[Note: actual dates will be specified in the final BPA.]

1.7 Administration

The Contractor is responsible for managing and successfully performing, completing, and delivering the obligations as ordered through this PWS and any Call Orders placed against this BPA, subject to the overall direction of the Government.

1.7.1 Place of Performance

The Contractor Services shall be performed on-site at multiple DHA Government Continental United States (CONUS) and some potential Outside Continental United States (OCONUS) locations. Locations where services are to be provided are described in Attachment 5 (Facilities Receiving Services).

1.7.2 Time of Performance

The Contractor shall provide the resources necessary to perform the Contractor Services in accordance with any applicable time schedules set forth in this PWS and any Call Orders placed against this BPA.

The Contractor is responsible for conducting business in adherence with this PWS and any Call Orders placed against this BPA. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS and any Call Orders placed against this BPA. When hiring personnel, the Contractor shall support and enable the stability and continuity of the workforce.

The Contractor shall promptly notify the Government upon becoming aware of any circumstances that may reasonably be expected to jeopardize the timely and successful completion (or delivery) of any Contractor Service. The Contractor shall use industry best practices and reasonable efforts to avoid or minimize any delays in performance and will promptly inform the Government of the steps the Contractor is taking or will take to do so, and the projected actual performance (or delivery) time. This notification does not constitute an acceptable delay in schedule unless approved by the Contracting Officer.

1.7.3 Manner of Performance

The Contractor shall perform the Contractor Services in compliance with this PWS and any Call Orders placed against this BPA and, in cases where a PWS does not prescribe or otherwise regulate the manner of the Contractor's performance of the Contractor Services, in accordance with industry best practices.

1.7.4 Emergency Services

On occasion, services may be required to support an activation or exercise of contingency outside the normal duty hours defined within Call Orders. The Contractor shall provide such immediate assistance and increased support as requested by the Government in relation to the management, containment, and resolution of any such contingency. As such, the Contractor shall coordinate the management, containment, and resolution of any crisis across the Integrated Services, and the planning and coordination of any restoration of the end-to-end services within the EITS Environment.

1.8 Costs

The Contractor shall bill for Contractor Services in accordance with any Call Orders placed against this BPA.

1.8.1 Other Direct Costs

The Contractor shall bill Call Order Other Direct Costs (ODCs) on a cost reimbursable, no-fee basis. ODCs are the purchase price of materials or services plus General and Administrative charges or Material and Handling charges. These costs must be preapproved by the COR and includes costs applied to the applicable Call Orders. All Call Order ODCs shall be fully supported in compliance with all requirements of the FAR, specifically Part 31. All ODCs shall be reported in the Monthly Progress Report as described in Exhibit 3 (Reporting and Service Level Management).

ODCs include but are not limited to auxiliary software and technical items that augment the delivery of Contractor Services (e.g., certain technical services, equipment, EUDs, cables).

The Contractor shall submit a request prior to procurement of non-travel ODCs to the Contracting Officer's Representative (COR) for approval. The ODC Approval Request shall include a description of the item(s) to be procured, the part number if applicable, identification of the sources and prices found with the recommended source highlighted, the quantity of each item to be procured, a total price prior to the application of Contractor indirect rates, the total indirect costs, a total price, and the delivery date. If the delivery date is expedited, resulting in additional or greater cost, a rationale shall be provided. After Government approval, the contractor shall be responsible for procuring and ensuring delivery and receipt of the items procured. After items have been procured and received, a detailed invoice with a breakdown of expenses shall be submitted to the COR.

1.9 Government's Contracting Officer Representative

The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notifies both the CO and Contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of Contractor Personnel. A letter of designation issued by the CO to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract.

1.10 Government Quality Assurance

The Government will evaluate the contractor's performance in accordance with the Quality Assurance Surveillance Plan (QASP) for Contactor Services. This plan provides a systematic method for the Government to evaluate performance and to ensure that the Contractor has performed in accordance with the performance standards detailed in the individual Call Orders. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable threshold levels or defect rate(s). Government may update the QASP and adopt new or different surveillance methods at its sole discretion.

PART 2
2.0 DEFINITIONS, ACRONYMS, AND APPLICABLE PUBLICATIONS/INSTRUCTIONS

2.1 Definitions and Acronyms

As described in Exhibit 1 (Definitions and Acronyms).

2.2 Applicable Publications and Administrative Instructions

The following publications and instructions are applicable and are periodically updated. The Contractor shall ensure it has access to the most recent publication.

The Contractor must abide by all applicable laws, regulations, policies, and procedures, including but not limited to:

2.2.1 Statutes

- Privacy Act of 1974, (5 U.S.C. 552a eq. seq)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996 and subsequent legislation
  https://www.hhs.gov/regulations/index.html
- Health Insurance Portability and Accountability Act of 1996 (Privacy Rule) effective October 15, 2002
- Health Insurance Portability and Accountability Act of 1996 (Security Rule) effective April 21, 2003

2.2.2 Department of Defense publications and instructions

The DHA documents (info.health.mil) are only available from within the Government network and will be accessible after award.

- DHA Contractor Training Instructions
- DHA Administrative Instructions (DHA-AI)
    - DHA-AI 074 Workforce Training Pursuant to the Requirements of the Privacy Act and the Health Insurance Portability and Accountability Act
      https://info.health.mil/cos/admin/privacy/Training%20Awareness/Training%20%20Awareness%20Library/2014-DHA%20AI%2074_WorkforceTrainingPolicy%20(2).pdf
    - DHA-AI 003, Physical Security Program
- DHA-PI
    - DHA-PI 8140.01 Acceptable use of DHA Information Technology (IT)
      https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Acceptable%20Use%20of%20DHA%20Information%20Technology%20(IT).pdf
    - DHA-PI 8160.01 Defense Health Program (DHP) System Inventory Management and Reporting

https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Defense%20Health%20Program%20(DHP)%20System%20Inventory%20Management%20and%20Reporting.pdf

- DHA-IPM
    - DHA-IPM 18-007 Service Delivery Management Program (EXTENDED) https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Service%20Delivery%20Management.pdf
    - DHA-IPM 18-009 Military Health System (MHS Enterprise Architecture-(EXXTENDED) https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Military%20Health%20System%20(MHS)%20Enterprise%20Architecture-(EXTENDED).pdf
    - DHA-IPM 18-010 Medical Community of Interest Circuits (EXTENDED) https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Medical%20Community%20of%20Interest%20Circuits%20(EXTENDED).pdf
    - DHA-IPM 18-015 Cybersecurity Program Management (Updated) (EXTENDED) https://info.health.mil/cos/admin/pubs/DHA%20Publications%20Signed/Cybersecurity%20Program%20Management%20(Updated)%20(EXTENDED).pdf
- DoD Instructions (DoDI)
    - DoDI 8510.01, Risk Management Framework (RMF) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf?ver=2019-02-26-101520-300
    - DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852002p.pdf
    - DoDI 8520.03, Identity Authentication for Information Systems https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf?ver=2019-02-26-101529-723
    - DoDI 8551.01, Ports, Protocols, and Services Management (PPSM) https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/855101p.pdf?ver=2019-02-26-101525-833
    - DoDI 8582.01, Security of Unclassified DoD Information on non-DoD Information Systems https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/858201p.pdf
- DoDD 8140.01, Cyber Workforce Management (2015) http://www.dtic.mil/whs/directives/corres/pdf/814001_2015_dodd.pdf
- DoDM 8570.01-M, Information Assurance Workforce Improvement Program https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program

https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897

2.2.3 Other publications

- Information Technology Infrastructure Library (ITIL) 4
  https://www.axelos.com/itil-4
- Committee on National Security Systems Instruction (CNSSI) 1253
- National Institute of Standards and Technology (NIST) Special Publications (SP)
  - NIST SP 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
  - NIST SP 800-53A Rev 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf
  - NIST SP 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations (RMF)
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
  - NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
    https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf
  - NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
    https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

PART 3
3.0 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3.1 Government Furnished Services

The Government will provide IT services necessary to maintain government issued equipment on Government furnished networks. The Government will provide remote access capabilities for Contractor's remotely accessing the Med-COI.

3.1.1 Government Provided Training

The Government will provide the training as required PWS and any Call Orders placed against this BPA for Contractor Personnel during contract duty hours. Contractor Personnel shall complete the training as per the mandatory training schedule. This training will typically encompass matters of security, safety, and other subjects. Contractor Personnel shall provide proof of required training to the COR in accordance with Part 5 section 5.1.3 EITSI Personnel Management.

3.2 Facilities

The primary places of performance for Contractor Services are in Government facilities as described in Part 1 section 1.7.1 Place of Performance. To the extent the Contractor utilizes Government Facilities to provide the Contractor Services, the Contractor's use of the Government Facilities will be for the sole and exclusive purpose of providing the Contractor Services and will be subject to the terms set forth in this PWS and any Call Orders placed against this BPA.

For Contractor Personnel working on-site at Government Facilities, the Government will provide commercially standard workspace for each individual to perform work, as well as access to any required office equipment (e.g., printer, copier). The Contractor shall be responsible for addressing, in its discretion and at its cost, any requests by such on-site Contractor Personnel for additional workplace accommodations, which will be appropriately discussed and coordinated with Government or other Customer, as applicable.

The Government may immediately remove any Contractor Personnel from any Government Facilities, as deemed appropriate, including if the person endangers the mission, is threatening or abusive, commits a crime, engages in an act of dishonesty while performing Contractor Services or violates Government's policies pertaining to safety, security, or use of Government Facilities or the data privacy and protection obligations under this PWS and any Call Orders.

The Contractor shall use the Government Facilities in an efficient manner and in a manner that does not interfere with Government's normal operations. The Contractor shall keep the Government Facilities in good order, not commit or permit waste or damage to them or use them for any unlawful purpose or act or any purpose other than the provision of the Contractor Services. The Contractor shall comply with Government's standard policies and procedures and all security requirements regarding access to and use of the Government Facilities, including procedures for the physical security of the Government Facilities. The

Contractor is responsible for any damage to Government Facilities resulting from its use of the Government Facilities.

The Contractor shall permit the Government and its agents and representatives to enter any portions of the Government Facilities occupied by Contractor Personnel at any time. The Contractor may not make improvements or changes involving workspace configuration, structural, mechanical, or electrical alterations to the Government Facilities without Government's prior written approval. Any improvements to the Government Facilities will become the property of Government.

When Government Facilities are no longer required for performance of the Contractor Services (or at the end of the applicable BPA term, whichever is shorter), the Contractor will return them to Government in substantially the same condition as when the Contractor began use of them, subject to reasonable wear and tear. Government may add, remove, or change Government Facilities.

3.3 Utilities

For work performed within Government Facilities, the Government will provide access to any utilities reasonably required in the performance of this contract. The Contractor shall instruct employees in utilities conservation practices, and shall be responsible for operating under conditions that preclude the waste of utilities.

3.4 Equipment

The Government will provide laptop computers as necessary to perform the tasks specified in this PWS. For work performed within government facilities, the Government will provide access to printers, scanners, shredders, and telephones for business purposes only. The Contractor is responsible for any damage to Government Furnished Equipment resulting from its use of the GFE outside of reasonable wear and tear.

3.4.1 Government Furnished Equipment Reporting

The Contractor shall maintain accountability for GFE issued to Contractor Personnel against the Government inventory accounting system (e.g., Defense Medical Logistics Standard Support (DMLSS).

Contractor shall track the GFE inventory information, at a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if Contractor-Acquired-Government Owned Property), and contract/order number under which the equipment is being used.

The Contractor shall report on the GFE within three Business Days of Government request.

3.4.2 Return of Government Property

Upon the completion of Contractor Services, or as directed by the Government, the Contractor shall return to Government (or applicable Customer), any equipment or other property of Government (or applicable Customer) if not previously returned, in condition at least as good as the condition when made available to Contractor, ordinary wear and tear excepted.

3.5 Materials

None.

3.6 Software

The Government will provide software licenses for the Contractor's use in delivering the Contractor Services identified in this PWS or any Call Orders placed against this BPA. Refer to Part 5 section 5.2.7 Service Management Systems for information on the major software systems in the EITS Environment.

PART 4
4.0 CONTRACTOR FURNISHED ITEMS AND SERVICES

4.1 General

The Contractor shall furnish all supplies, equipment, software, facilities, and services required to perform the work of this PWS and as described in any Call Order PWSs, other than those specified in Part 3.

4.2 Facilities

The primary place of performance for Contractor Services are in Government facilities as described in Part 1 section 1.7.1 Place of Performance.

Where required by a Call Order, the Contractor shall provide the facilities and facilities-related support it needs to provide the Contractor Services. Such facilities shall be in the United States, unless specifically directed by the Government otherwise.

The Contractor may be required to perform under this PWS and any Call Orders placed against this BPA at contractor or other facilities when Government space is not available or during contingency situations. The contractor may be required to provide necessary workspace for the contractor staff to provide the support outlined in the PWS to include desk space, telephones, computers, and other items necessary to maintain an office environment.

4.2.1 Secret Facility Clearance

In accordance with standard form DD 254, the Contractor shall possess and maintain a SECRET or higher Facility Clearance Level (FCL) from the Defense Counterintelligence and Security Agency (DCSA). If a subcontractor or teaming partner to Contractor has no FCL or an FCL lower than the required classification level indicated, the Contractor must sponsor its subcontractor or teaming partner for a new FCL or an FCL upgrade.

4.3.1 Utilities

Except as expressly provided under Part 3 of this PWS, the Contractor is responsible for providing all utilities (e.g., electricity, water, gas, phone, network) in the facilities it utilizes.

Contractor shall provision and maintain all necessary telecommunications connectivity and manage that connectivity to meet the designated performance standards.

4.4 Equipment

Except as expressly provided under Part 3 of this PWS, the Contractor is responsible for providing the equipment, materials, and related support it needs to perform Contractor Services of this PWS and any Call Orders placed against this BPA.

4.5 Materials

The Contractor shall furnish all materials not listed under Part 3 of this PWS required to perform work.

4.6 Software

Except as expressly provided under Part 3 of this PWS, the Contractor shall provide all software, licenses, and rights to use for software, to perform the integrated services identified in this PWS and any Call Order PWSs. Software and other solutions installed on GFE must be approved in advance and shall go through the ATO process prior to installation.

PART 5
5.0 SPECIFIC TASKS

Table 1: EITSI Scope by Objectives and Tasks

5.1 Contract Management

The Contractor shall provide management to ensure contract performance is efficient, accurate, on time, and in compliance with the requirements of this PWS or any Call Orders placed against this BPA.

5.1.1 EITSI Contract Compliance

The Contractor shall ensure performance of all tasks are in compliance with applicable Federal and DoD policies and regulations, including but not limited to those listed in the BPA, this BPA PWS, and any Call Orders.

5.1.2 EITSI Deliverables Management

The Contractor shall track the status of all Deliverables, including required submission timeframes, approvals, rejections, revisions, and all other actions related to successful completion of deliverables.

5.1.2.1 Deliverables Schedule

The Contractor shall adhere to the schedule of Deliverables in Call Orders as identified in Call Order PWS.

5.1.2.2 Software-Related Deliverables

The Contractor shall adequately and comprehensively test any software-related Deliverables prior to providing them to Government. Software Deliverables will be provided in both Source Code and object code forms.

5.1.2.3 Review of Deliverables

Upon the Contractor submission of a Deliverable and certification that the Deliverable complies in all material respects to the technical, design, and functional specifications, Government may review and test such Deliverable to determine whether it is free from errors and defects and meets any applicable Acceptance Criteria. Call Orders may set forth the specific procedure for review and testing by Government of each Deliverable.

5.1.2.3.1 Deliverable Review Period

The Review Period for each Call Order Deliverable will be thirty (30) days after delivery, unless otherwise specified by the Government in the Call Order. The Contractor will assist Government as Government reasonably requires in review and testing, including by cooperating with the efforts, providing a technical environment to facilitate such review, and providing applicable documentation and information that may assist in such review and testing.

5.1.2.3.2 Deliverable Review Statement

Prior to the expiration of the applicable Review Period, Government will provide the Contractor a written statement indicating Acceptance or rejection of the Deliverable.

Acceptance will occur only through a written statement. In no event will a Deliverable be deemed to be Accepted by Government, even where payment is made for the Deliverable, or the Deliverable is used in production, or any other basis, where there has been no issuance of a written statement.

5.1.2.4 Revision of Deliverables

If the Contractor receives a written statement indicating Rejection of a Deliverable, the Contractor shall provide a proposed resolution for correcting the deliverable within five (5) days. The proposed resolution shall indicate the Contractor's plan to correct the Deliverable so that no Non-Conformities remain within ten (10) days (unless a different time period is agreed to by the Government) of Government's approval of the proposed resolution. Upon the Contractor's revision or correction of the Deliverable, the Contractor will provide Government with the revised Deliverable, whereupon the acceptance testing procedure and timetable set out in this Section 5.1.2 Deliverables will be repeated.

5.1.2.4.1 Revision after Acceptance

In the event of a discovery of a defect in a previously Accepted Deliverable, where such defect would have qualified as a Non-Conformity at the time of Acceptance, upon notification by Government or the applicable Customer, the Contractor shall, at no additional charge, repair or replace or otherwise correct the Non-Conformity to the level of performance specified in this BPA and any Call Orders. The Contractor shall conduct a revision of the deliverable as directed under 5.1.2.4 Revision of Deliverables.

5.1.2.5 Format

Unless specified otherwise in a Call Order, the Contractor shall submit Deliverables in the form of a Microsoft Office document, using the version in use by the Government at the time of submission, where such Deliverables, reports, and other documents are delivered to the Government outside of a system (e.g., Service Management System) by the Contractor as

part of Contractor Services. Deliverable formats and templates may be further specified in Call Orders.

5.1.2.6 Non-Proprietary

In no event, shall the Contractor submit any document or other deliverable for performance of Contractor Services marked "Proprietary."

5.1.3 EITSI Personnel Management

The Contractor shall provide management of personnel actions (e.g., recruit, train, retain, replace) necessary to staff qualified personnel to fulfil contract requirements.

The Contractor Personnel assigned to perform the Contractor Services will have appropriate skills, experience, and training to enable them to perform such Contractor Services in a professional and workmanlike manner, consistent with generally accepted industry standards. Throughout the term of this PWS and any Call Orders, the Contractor shall establish and maintain policies, procedures and training programs reasonably designed to assist Contractor Personnel in complying with the Contractor's duties and obligations under this PWS or any Call Orders placed against this BPA.

The Contractor shall manage, supervise, and provide direction to Contractor Personnel and cause them to comply with the obligations and restrictions applicable to the Contractor under this Agreement. The Contractor shall make Contractor Personnel aware of, and cause them to comply with, Government Rules, including safety and security policies applicable while performing Contractor Services at Government Facilities or accessing Government Data or Government Information Systems.

5.1.3.1 Removal and Replacement of Contractor Personnel

The Government may require the Contractor to remove any individual Contractor Personnel from the performance of Contractor Services if the Government reasonably determines with reason that the individual is not suitable to the Government work environment of the Contractor Services. Any such removal will be performed immediately following request from the Contracting Officer. The Contractor shall, unless the Contracting Officer requests otherwise, assign a replacement resource to the Contractor Services as soon as practicable.

5.1.3.2 Qualifications and Training of Contractor Personnel

The Contractor shall ensure personnel it assigns or utilizes in the performance of this contract meet the requirements of the roles to which they are assigned, including at a minimum, the experience, educational, security, and other requirements set forth in Exhibit 5.3 (Labor Role Descriptions) and Attachment 4 (Special Clearances and Certification Requirements) of this PWS and are fully capable of performing in an efficient, reliable, and professional manner.

The Contractor shall complete all requirements, training, and forms per DHA instructions. The DHA's Contractor training instructions will be provided as described in Part 7 section 7.1.3 DHA Contractor Training Instructions.

5.1.3.2.1 Contractor Personnel Onboarding Checklist

The Contractor shall comply with onboarding requirements of the DHA for Contractor Personnel requiring a Common Access Card (CAC), including DoD- and DHA-directed training and forms submission, prior to network access, as displayed in the In/Out-Processing Portal. Access to the In/Out Processing Portal will be provided post award.

5.1.3.2.2 Access Removal for Deficient Certification

The Contractor shall ensure that all Contractor Personnel have proper and current certifications for their roles and responsibilities in providing Contractor Services, and deny access to DoD information systems to personnel without such training and certifications.

5.1.3.3 Contractor Personnel Security

The Contractor shall comply with the security screening and background check requirements and processes as described in Part 6 section 6.1 Contract Work Classification.

5.1.3.4 Non-Disclosure Agreement (NDA)

All Contractor Personnel who will obtain access to proprietary, classified, or confidential information or any information release that is protected or governed by law or regulation associated with DHA acquisitions shall be required to complete and sign a DHA Contractor NDA (DHA Form 49) prior to beginning work on the subject contract. The Contractor shall execute an NDA on behalf of the company and shall ensure that all staff assigned to, including all subcontractors and consultants, or other personnel performing on Call Orders execute an NDA protecting the procurement sensitive information of the Government and the proprietary information of other contractors. The NDA shall be executed not later than first day of performance and renewed upon exercising a contract option period. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor. The Contractor shall maintain originally signed (wet signed or electronic signed) NDAs of individual employees and provide copies to the COR.

5.1.3.5 Contractor Personnel Identification

The Contractor shall ensure that Contractor Personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

5.1.3.5.1 Announcement

Contractor Personnel will be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this PWS or any Call Orders placed against this BPA. Contractor Personnel shall make their contractor status known during introductions.

5.1.3.5.2 Retired and Reserve Military Service Personnel

Contractor Personnel, while performing in a contractor capacity, are prohibited from using their retired or reserve component military rank or title in any written or verbal communications associated with the contracts in which they provide services.

5.1.3.6 Physical Security

The Contractor shall be responsible for safeguarding all government equipment, information, and property furnished for use by Contractor Personnel. Contractor shall comply with safeguarding in accordance with DHA-AI 003 Physical Security Program or local Government facility SOPs.

5.1.3.7 Key Control

The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor Personnel. The Contractor shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the CO.

Contractor shall establish and implement methods to ensure all keys and key cards issued to the Contractor by the Government are appropriately used, and are not lost, not misplaced, and not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the QCP. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer or their COR.

5.1.3.7.1 Common Access Card

The Contractor shall complete or provide to the Government all information required per the DHA Common Access Card (CAC) request process, current version 2.1, January 2018, or more recent when updated. See process attached in Part 7.1 of the PWS. A CAC is the standard identification for eligible DoD contractor personnel. The Contractor shall return all CACs to the COR upon the departure of the contractor personnel.

5.1.3.7.2 Key Loss

In the event keys, other than master keys, are lost or duplicated by the Contractor, the Contractor shall, upon direction of the CO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the payment due the Contractor. In the event a master key is lost or duplicated by the Contractor, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the payment due the Contractor.

5.1.3.7.3 Lock Combinations

The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations.

5.1.3.8 All Personnel Report

Contractor shall update and maintain a list of Contractor Personnel working under this PWS or any Call Orders placed against this BPA. Contractor shall track information for each Contractor Personnel as shown in the form for (Contractor Personnel List).

5.1.3.8.1 Emergency Rosters and Notifications

Contractor Personnel shall register themselves in the DHA emergency notification system.

5.1.4 EITSI Key Personnel

Certain Contractor Personnel positions shall be designated as "Key Personnel" positions, to be filled by approved Contractor Personnel in accordance with this section (each, a "Key Personnel"). The Key Personnel will be specified in any Call Order(s) against the BPA. The Government may, as required, change the particular positions that are designated as Key Personnel in subsequent Call Orders.

Contractor shall cause each of the Contractor Personnel filling each Key Personnel position (whether as of the Effective Date, or during the Term, including replacement Key Personnel) to be full-time dedicated to the provision of the Contractor Services, unless the Call Order expressly states otherwise with respect to the particular Key Personnel position.

Contractor shall ensure that Key Personnel are highly qualified and capable of fulfilling the responsibilities of their positions.

5.1.4.1 Change of Key Personnel

Contractor shall not transfer, reassign, or remove any Contractor Personnel from their Key Personnel position (or announce its intention to do so) without Government's prior written approval. The Government may withhold any such approval if it is not in the Government's interest.

In connection with any change in Key Personnel, the Contractor shall:

- Give Government, at least sixty (60) days advance notice of a proposed change in Contractor Personnel filling a Key Personnel position (and where sixty (60) days is not possible, as much advance notice as is possible);
- Within thirty (30) days of the notice, obtain Government's approval of a suitable replacement, and have that Key Personnel replacement performing; and
- Arrange (unless the circumstance of such change prevents) for the proposed replacement Key Personnel to work side-by-side with the incumbent Key Personnel during the notice period to affect a seamless transfer of knowledge prior to the incumbent leaving the Key Personnel position.

5.1.4.2 Government Review of Key Personnel

Before assigning a Contractor Personnel as a Key Personnel, whether as an initial or subsequent assignment, the Contractor shall notify Government of the proposed assignment, and provide Government a resume and other information about the individual and their background and experience.

If Government objects to the proposed assignment, the Contractor shall not assign such individual to that position and shall propose another Contractor Personnel of suitable ability and qualification, in accordance with the foregoing.

For the purpose of the Contractor's performance management of Key Personnel, the Contractor shall, at Government request, hold an annual joint session with Government to review program goals and objectives as well as to receive feedback relative to the past year's performance.

5.1.4.3 Contract Program Manager

Contractor shall provide a contract Program Manager (PM) who shall be responsible for the performance of Contractor Services. The Program Manager or alternate shall have full authority to act for the Contractor on all contract matters relating to daily operation of this contract and the delivery of Contractor Services. The Government expects the Program Manager to be required in all Call Orders.

The Program Manager will be deemed a Key Personnel and shall conform to the Key Personnel provisions, including length of assignment. The Contractor shall ensure the Program Manager:

- Will be the primary point of accountability for the Contractor in dealing with Contractor Services delivery under this Agreement, except in cases where the Government agrees that other Contractor Personnel will act as points of contact with Government with respect to specifically identified subject matter or areas,
- Will have overall responsibility for managing and coordinating the delivery of the Contractor Services, including for customer satisfaction and Service Level attainment,
- Will meet regularly with the designated Government representatives at designated Government facility(ies)
- Will have the power and authority to make decisions with respect to actions to be taken by Contractor in the ordinary course of day-to-day performance of the Contractor Services in support of Government's EITSI program in accordance with this PWS.

5.1.4.4 Key Personnel Positions

The staff roles that will be identified in Call Orders as Key Personnel may include, but will not be limited to:

Role	Description
Program Manager	As described in 5.1.4.3, this individual is charged with managing and coordinating the delivery of Contract Services. This role is the highest Contractor point of contact assigned to this BPA.
Transition Project Manager	For the period of Transition-In, this role is accountable for implementation performance and governance, including addressing issues and risks in implementation.

Role	Description
Chief Operations Manager	This role has oversite of all operations for delivery of Contractor Services, including the practices for Event, Incident, Problem, Change, and Service Request. This role leads the EITSI use of SMS and compliance with the SMM.
Program Management Functions Manager	This role leads the Program Management Functions and use of the Project and Portfolio Management SMS for all the Integrated Service Providers. This role provides oversight for On-Going Programs. This role manages the EITSI personnel conducting the Solution Request Management practice, the Service Portfolio Management practice, and the Project Management practice.
SMM Manager	This role is responsible for planning and implementing the SMM; including its overall taxonomy, organization, and management. This role is responsible for the On-Going Program for SMM Currency, the continual maturity of the SMM, and the drive to single processes in the EITS Environment. This role drives all the Integrated Service Providers for adoption, participation, and compliance with the SMM.
Organizational Change Manager	This role drives the practice of Organizational Change for the EITSI and Integrated Service Providers. This role is responsible for communication, coordination, and training across the EITS Environment and is accountable for accomplishing the smooth transition of initiatives in establishing the full vision for the EITS program.
Continual Improvement Manager	This role drives Continual Improvement activities in the EITS Environment across all the Integrated Service Providers, and manages the EITSI effort for the Continual Improvement practice. This includes aligning EITSI practices with the derived and expected value to the MHS mission.
Chief Architect	This role manages the EITSI effort for the practice of Architecture Management in the EITS Environment, including the On-Going Program of Technology Planning. This role serves as the primary liaison to the DHA ESA-BAD.
Chief Security Architect	This role is responsible for the Information Security Management and Risk Management Framework practices, including the On-Going Program of Security Planning. This

Role	Description
	role coordinates cyber security and risk management activities across the Integrated Service Providers, including adherence to security policies and compliance. This role serves as the primary liaison to DHA Cyber Security Division (CSD) for the EITS Environment.
Service Level Performance Manager	This role is charged with measuring and reporting on the quality of service delivery across all the Integrated Service Providers, and initiating Problem items and Continual Improvement items to protect and improve the quality of delivery. This role leads the EITSI effort for the Service Level Management practice in the EITS Environment, and is charged with creating and managing the Quality Management Plan.
Governance Forum Lead	This role coordinates and facilitates EITS Governance for the Integrated Service Providers. This role ensures that the obligations of EITS Governance are met. This role facilitates rapid issue resolution and the dissemination of decision making in EITS Governance.
Customer Relationship Manager	This role leads the Business Relationship Management function for the EITSI, and supports Customer interactions across the Integrated Service Providers. This role supports and coordinates the On-Going Program of Customer Satisfaction, and manages the Business Analysis and Demand Management practices for the EITSI to advocate and serve Customers and the overall MHS mission.
Service Provider Relations Lead	This role leads the Integrated Service Provider Management function for the EITSI and has primary relationships with the various Integrated Service Providers. This role facilitates and coordinates the development of OLAs and the currency of OLAs across the Integrated Service Providers.

Key Personnel positions required for Call Orders will be specified in the Call Order PWS. Required qualifications for Key Personnel are as described in Exhibit 5.3 (Labor Role Descriptions).

5.1.5 EITSI Reporting Management

5.1.5.1 Reporting Status

The Contractor shall develop monthly status reports based on requirements outlined in this BPA PWS and Call Order PWSs. The monthly reports shall include accomplishments during

the reporting period, planned activities for the next reporting period, current status of risks and issues, and other relevant information which must be reviewed and discussed. The Contractor shall provide status reports and in-person briefings in accordance with Call Order requirements. Contractor may be required to present this information in different formats to include in-person briefings.

Contractor shall provide reporting on the delivery of Contractor Services as described in Exhibit 3.3 (Report Matrix).

5.1.5.2 Service Levels

The Contractor's level of performance will meet the performance standards designated as Service Levels in Exhibit 3.1 (Service Level Matrix) as specified.

5.1.5.2.1 Measuring and Reporting Service Levels

The Contractor shall implement and utilize the necessary measurement and monitoring tools and procedures required to measure and report the Contractor's performance of the Contractor Services against the applicable Service Levels. Such measurement and monitoring will permit reporting at a level of detail sufficient to verify compliance with the Service Levels, and will be subject to Government verification. The Contractor will provide Government with information and access to such tools and procedures upon request, for purposes of verification. In addition, the Contractor will make available to Government any data in the Contractor's possession regarding measurements taken by the Contractor with respect to any Service Levels.

5.1.6 EITSI Schedule Management

As part of any Call Order, the Contractor shall develop and maintain a master schedule of all major activities, tasks, and milestones. This master schedule shall identify and track interdependencies with third party schedules (e.g., Government and other vendor schedules).

5.1.7 EITSI Travel Management

The Contractor shall be required to travel Continental United States (CONUS) to attend meetings, conferences, and training, or for other purposes as directed by the Government under Call Orders. Minimum OCONUS travel may be required as requested in Call Orders. . Specific OCONUS requirements will be established and negotiated in Call Orders as required. The Contractor may be required to travel to off-site training locations and to ship training aids to these locations. Contractor shall be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation and the limitation of funds specified in this contract. All travel requires Government approval and authorization, and notification to the COR. Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred, billed, and reimbursed in accordance with FAR Part 31.

5.1.7.1 List of Sites for Travel

Locations which potentially may require travel are listed in Attachment 5 (Facilities Receiving Services). Call Orders may include additional sites.

5.1.7.2 Contractor Foreign Travel

OCONUS travel is in the scope of this BPA. Specific OCONUS requirements will be established in Call Orders as required.

The Contractor shall ensure that assigned participants allow sufficient lead-time to obtain valid passports, country clearances, and immunizations to support project activities. The Contractor shall travel using the lower cost mode of transportation commensurate with the mission requirements. Lodging shall be reimbursed in accordance with approved per diem rates for the destination city.

The Contractor shall perform OCONUS travel in accordance with Status of Forces Agreements (SOFAs). Specific SOFAs, Expatriation and Repatriation Costs will be provided with any relevant Call Orders.

5.1.9 EITSI Quality Management

The Contractor shall maintain an effective quality management program to ensure services are performed in accordance with the standards identified in this PWS or any Call Orders placed against this BPA PWS and any Call Order PWSs. The Contractor shall implement procedures to identify and prevent quality issues, and to correct these issues if they occur.

5.1.10 EITSI Transition Management

5.1.10.1 Planning

Where required by Call Orders, the Contractor shall create, and obtain Government approval of, a detailed **Transition-In Plan** addressing the transition and implementation of Contractor Services. The Contractor shall update and report on the Transition-In Plan weekly until Contractor Services are fully deployed.

As requested as part of a Call Order, the Contractor shall create, and obtain Government approval of, a written **Transition-Out Plan** addressing the transition of Contractor Services, in whole or in part, away from the Contractor to a Government designee.

5.1.10.2 Transition-In

The period between the award date and full performance start date of a Call Order constitutes the Transition-In period, which will be specified in the Call Order PWS. During the Transition-In period, the Contractor shall prepare to meet all contract requirements and ensure incoming personnel are functionally trained and qualified on the full performance start date.

5.1.10.2.1 Transition-In Plan

Transition-In plans may include, but are not limited to:

- Coordination with Government representatives
- Review, evaluation, and transition of current support services
- Transition of historic data to new Contractor system
- Government-approved training and certification process
- Establish credentials for Contractor Personnel and for the transition of other credentials

- Transfer of hardware warranties and software licenses (if applicable)
- Transfer of all necessary operations and technical documentation
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable)
- Orientation phase to introduce Government personnel and users to the Contractor's team, tools, methodologies, and business processes
- Distribution of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable DHA briefing and personnel onboarding procedures
- Coordinate with the Government to account for Government keys, ID/access cards, and security codes

5.1.10.2.2 In-Process Work Activities

Upon the Commencement Date, Contractor shall assume responsibility for continuing the development, implementation, and support of current projects and in-process requests for services as identified by Government without material interruption and either (i) in accordance with then current written Government plans for such current projects and in-process requests for services, if such plans exist and have been furnished to Contractor, or (ii) if no such written plans have been furnished to Contractor, as such current projects and in-process requests for services are being performed as of the Commencement Date.

During the implementation of Contractor Services, the Government and Contractor will review the then current work activities and other in-process work (e.g., requests for services). Contractor shall create and maintain a list of these work activities up through the time it assumes responsibility for services. The Government will determine the work activities and other in-process work which will become the Contractor responsibility and a date by which Contractor shall assume that responsibility.

Contractor shall complete all such work activities and in-process work in accordance with the following:

- DAD IO/J-6 Change management procedures to address any changes in scope, requirements, schedules, or cost with respect to the in-process work
- DAD IO/J-6 Solution Request and proposal processes in place as of the date the Contractor is to assume responsibility
- DAD IO/J-6 Project management and development practices in place as of the date the Contractor is to assume responsibility for these projects

Within ninety (90) days after the Commencement Date, Contractor shall provide the Government with a written evaluation and assessment of the status of all current projects and in-process requests for services known to Contractor.

5.1.10.3 Transition-Out

Transition-Out performance will be in accordance with individual Call Orders. Transition may be to a Government entity, another Contractor under contract, or to the incumbent Contractor under a new contract. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition

from this Contract and any Call Orders issued under this Contract to a successor provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of items such as copies of existing policies and procedures, and delivery of required metrics and statistics.

Contractor shall provide Transition-Out Assistance to the Government, as directed in any Call Orders.

The quality of the Contractor Services provided by the Contractor, and the Contractor's performance of the Contractor Services, including the affected Contractor Services, will not be degraded during the Transition-Out Assistance period. Except as approved by the Government, the Contractor will not make any changes to the number of Contractor Personnel providing Contractor Services during the Transition-Out Assistance period or reassign Contractor Personnel away from performing Contractor Services under this contract during the Transition-Out Assistance period. Transition-Out Assistance will include the assistance and obligations, as requested by Government, described in the Transition-Out Plan.

5.1.10.3.1 Transition-Out Plan

Transition-Out plans may include, but are not limited to:

- Coordination with Government representatives
- Review, evaluation, and transition of current support services
- Transition of historic data to new Contractor system
- Government-approved training and certification process
- Transfer of hardware warranties and software licenses (if applicable)
- Transfer of all necessary operational and technical documentation
- Transfer of compiled and un-compiled source code, to include all versions maintenance updates and patches (if applicable)
- Orientation phase to introduce Government personnel and users to the Contractor's team, tools, methodologies, and business processes
- Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, and computer equipment
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable DHA debriefing and personnel out-processing procedures
- Turn-in of all Government keys, ID/access cards, and security codes

5.1.10.3.2 Transition-Out Assistance

As part of the Transition-Out Assistance, Contractor shall provide all assistance as Government may reasonably request to transition the affected Contractor Services to Government or its designee.

5.1.10.3.2.1 General Support

To the extent requested, Contractor shall:

- Assist Government or its designee(s) in updating and detailing the Transition-Out Plan as appropriate to affect the specific disengagement

- Perform configuration and consulting services to assist in implementing the Transition-Out Plan
- Train personnel designated by Government or its designee(s) in the use of any business processes, work instructions and work procedures, and any equipment, software, systems, materials, and tools used in connection with the performance of the affected Contractor Services
- Document and create a catalog all business processes, work instructions, work procedures, software, Government Data, equipment, materials, third party contracts, and tools used to provide the affected Contractor Services
- Provide machine readable and printed listings and associated documentation for Source Code for software owned by Government or any other Customer and Source Code to which Government or any other Customer is entitled under this contract and assist in its re-configuration
- Provide technical documentation for Software used to provide the affected Contractor Services
- Assist in the execution of a parallel operation, data migration, and testing process until the successful completion of the transition of the affected Contractor Services to Government or its designee(s)
- Create and provide copies of the Government Data related to the affected Contractor Services in the format and on the media reasonably requested by Government and/or its designee(s)
- Provide a complete and up-to-date, electronic copy of the SMM and applicable business processes, work instructions and work procedures in the format and on the media reasonably requested by Government
- Provide other technical assistance requested by Government that is reasonably related to the disengagement with respect to the affected Contractor Services

All Transition-Out Assistance shall be provided subject to and in accordance with the terms and conditions of this contract, including Service Levels.

5.1.10.3.3 BPA Closeout

Prior to the expiration or scheduled termination date of this BPA, Contractor may be provided close out documentation and shall complete, sign, and return to Government within thirty (30) days of receipt. Any closeout documentation not received within thirty (30) days of Contractor's receipt of the Government's request will be documented in the contract file as Contractor non-compliance.

5.2 Integrated Environment

The Contractor shall function as the EITSI, and provide integration for the EITS Environment. Within the EITS Environment the Contractor shall be responsible for:

- Coordinating and implementing policies, processes, and procedures across the Integrated Service Providers for all Integrated Services, and ensuring the documentation of policies, processes, and procedures in the SMM
- Integration of processes across the Integrated Service Providers and Customers
- Validating compliance with processes

- Managing OLAs and compliance with OLAs across the processes documented in the SMM
- Coordinating the operation of the Service Management Systems (SMS) (e.g., ITSM system)
- Facilitating the service integration and use of Service Management Systems by the Integrated Service Providers and Customers.
- Coordinating Service Level Management and reporting

The Contractor shall manage the Integrated Environment based on the IT service management practices in the ITIL 4 framework, which focuses on adaptability and value creation, along with the traditional best practices of the service management life cycle and the linkages between service management components:

- Implement and maintain processes for the Integrated Environment based on the practice areas for ITIL 4 (i.e., General IT Management Practices, Service Management Practices, and Technical Management Practices)
- Implement other practices (e.g., CMMI) where such practices support the mission need of DHA and Customers

5.2.1 Integrated Service Provider Management

The Contractor shall manage and coordinate the delivery of Integrated Services by the Integrated Service Providers in compliance with this PWS and any Call Orders. Contractor shall assist the Government with oversight of the Service Providers and EITS Governance.

The Contractor shall integrate the practices of Service Providers, Customers, and other vendors, where the practices interact. Contractor shall integrate processes to support the Integrated Environment with Service Providers, Customers, and other vendors, where the processes interact.

The Contractor shall coordinate activities across all functions and organizations, including the Integrated Service Providers, Customers, and other vendors, that provide services and Integrated Services to Customers. Contractor shall communicate and coordinate the associated policies, processes, sub-processes, and procedures of the Integrated Environment, across the Contractor's organization, the Integrated Service Providers, and designated other vendors.

The Contractor shall facilitate and coordinate information exchange between and among Contractor, the Service Providers, Customers, and other vendors to improve the execution of the Integrated Environment responsibilities. Contractor shall ensure that the Integrated Environment permits flexibility and facilitates effective communication across functions, Integrated Service Providers, Customers, geographic regions, and other vendors.

The Contractor shall manage the integrated delivery of the Service Providers in the best interests of the Government. That management is as directed by the Government, and shall include, but is not limited to:

- Establish OLAs with Service Providers
- Collect and report service levels and key measure details from Service Providers
- Work with Service Providers where the Government or Customers report that Customers are experiencing performance problems

- Establish acceptable methods of communication with Service Providers and other vendors to plan, resolve issues, mitigate risks, and resolve disputes
- Manage the involvement of Service Providers in the portfolio of projects
- Recommend replacement or addition of Service Providers and work with Government to develop supporting materials for any acquisitions.
- Coordinate the development of new and changed services with Service Providers
- Monitor business changes in the Service Provider organizations and identify impact on the Integrated Environment and report those to Government

The Contractor shall ensure and validate that the Integrated Environment provides an audit trail that meets all Government policies and regulations.

5.2.1.1 Deliverables Management for Service Providers

The Contractor shall track the deliverables from the Service Providers. Contractor shall ensure that all deliverables have a documented deliverable definition and acceptance criteria approved by the Government. Contractor shall facilitate the Government's review and Acceptance of Service Provider deliverables.

Contractor shall track the production, submission, review, and Governmental approval of Service Provider deliverables. Contractor shall provide a system for tracking that is appropriately controlled to be available solely to the Government, the Service Provider, and certain EITSI personnel.

5.2.1.2 Quality Assurance for Service Providers

The Contractor will implement processes and supporting measures and operate Quality Assurance across the Integrated Services to improve mission aligned IT service quality. The Contractor will employ a Quality Assurance (QA) program, tools, and processes as approved by the Government.

The Contractor shall develop and employ a Quality Assurance program, designed to promote performance of the Services to optimize Overall Program Measures and EITS mission results. Contractor will focus on measuring and improving quality, reliability, speed, cost-effectiveness, security, the customer experience, and Customer satisfaction.

The Contractor shall design, document, implement, and maintain procedures, processes, and measurements in the SMM for all Quality Assurance activities across the Integrated Services. Contractor shall verify and document ongoing compliance with the Quality Assurance program, procedures, and standards by the Integrated Service Providers.

The Contractor shall test results, validate test results, determine level of improvement and report findings to the Government.

5.2.2 EITS Governance

The Contractor shall provide analysis and recommendations for the governance of the delivery of IT services within the EITS Environment as requested by the Government.

Contractor shall work with the Government on the development of the EITS Governance framework as described in 1.3.3.2 EITS Governance Framework. The development of the framework shall adhere to the following guiding principles:

- Strong and effective Customer engagement
- Resolving issues at lowest possible level
- Establishing representative groups to resolve issues
- Regularly validating and updating Operational Documents
- Monitoring contractual requirements
- Managing interparty relationships among all Integrated Service Providers
- Evolving service options and supporting innovation
- Formalizing roles and responsibilities for strategy and issue management among Government, Customers, and Integrated Service Providers
- Aligning management of IT-related risk with overall risk management

5.2.2.1 Coordination of Governance Forums

The Contractor shall support the Government-run Relational Forums. Contractor shall provide support and representation for the Integrated Service Providers as requested by the Government. Contractor shall disseminate decision making back to Operational Forums as required.

The Contractor shall establish Operational Forums as approved by the Government. Contractor will facilitate, coordinate, and conduct the Operational Forums. Contractor shall include Government representatives as requested by the Government.

The Contractor Personnel participating in forums are expected to be able to make recommendations for Government approval and resolve issues as appropriate for the level and purpose of that forum. Contractor shall report to the Government on all issues being worked and ensure that the accountability to the Government is preserved.

5.2.2.1.1 Governance Documents

The Contractor shall utilize the Document Data Store (see section 5.3.4.1) for all governance forums where the EITSI participates. Contractor shall appropriately secure the documents to the participants and stakeholders in governance, as approved by the Government. Contractor shall ensure governance documentation (e.g., minutes, agenda, decision briefings, and other artifacts) are stored in the designated document data store.

The Contractor shall produce minutes and agenda of all meetings where the EITSI participates. The minutes will include topics discussed, issues resolved, and open action items with responsible person's name and date to close.

The Contractor shall document decisions made and shall complete any follow up tasks, such as updates to associated artifacts, for the governance forums where the EITSI participates.

5.2.2.1.2 Governance Issue Management

The Contractor shall track and manage all issues in EITS Governance, in the designated SMS, as approved by the Government.

The Contractor shall coordinate with Customers and Integrated Service Providers involved in the issue to complete the required documentation for decision making and actioning. Such documentation shall include:

- Unique issue number
- Issue description, confirmed by the Government, as a statement of the facts in the situation
- Proposed issue resolution from relevant parties (Government, Customer, EITSI, service providers)
- Previous solutions attempted for resolution
- Other relevant details including, as applicable, cost implications, additional factual background, and contract references

The Contractor shall coordinate the distribution of the issue materials in support of the relevant forums in advance of the meeting, with appropriate time for review and input by the forum membership.

5.2.2.1.3 Issue Escalation

EITS Governance shall strive to resolve the vast majority of issues at the operational level. The EITSI is expected to facilitate the issue resolution processes, in accordance with other processes in the PWS and Call Orders and the SMM as applicable. However, not all issues will be resolved at the operational level, so the governance model will include an escalation process designed to promptly and efficiently escalate the issue for resolution.

Where the Government, the Customer, and Contractor determine an issue cannot be resolved at an operational level and it cannot be resolved with escalation to EITSI, the issue is escalated to the Relationship Forums.

5.2.2.2 EITS Governance Forums

The Government will identify certain governance forums that it expects to establish with the EITSI in this PWS and in any Call Orders.

The Contractor shall document and maintain information on all EITS Governance Forums in the SMM, which shall at a minimum include: charters, cadence, purpose, scope, participants, roles, authority and decision rights, escalation paths, reporting, other logistics, and key success indicators.

Although each forum has its own unique purpose and scope, there are interrelationships among them, including information sharing and escalation. In general, information sharing and escalation begins at the operational level, then to the management level and finally to the strategic level. The Contractor shall document the specific information sharing and escalation relationships within the processes for EITS Governance in the SMM.

5.2.2.2.1 Relational Forums (notional)

The initial Relational Governance Forums have been identified as:

- EITS Relationship Forum
  This provides for Customer engagement in decision making and directing the strategic direction of the EITS Environment, and in all ways is the primary voice of the Customer within the EITS Environment. This forum is chaired by the Government and supported by the EITSI, with Customer participation, and other participation as required. This forum has oversight of activities and EITS Environment initiatives for Customers, including the On-Going Programs. This

forum also reviews issues where they involve Customer decision making and direction, as determined by the Government.

- SP Relationship Forum
  There will be one of these forums for each Integrated Service Provider. Each of these forums provides for review and actioning of issues with the delivery of services from that Service Provider, where the issue cannot be resolved in the operational forums and the issue is determined to be approaching the bounds of the obligation of the PWS and any Call Order. This forum is chaired by the Government, with participation from the Service Provider, and other participants as required. The forum also reviews service performance metrics, service delivery plans, resource utilization, and provides general management, oversight, and review of the delivery of the Service Provider Services, where such items are not performing within the bounds of the Service Provider's obligations.

5.2.2.2.2 Operational Forums (notional)

Operational Governance consists of day-to-day management of the Integrated Services, issue resolution, and Customer-specific technology decisions. Success of the EITS Governance rests largely on managing Operational Governance, including resolving issues and making decisions, at the lowest possible level. Thus, the vast majority of issues are resolved through interaction among the Government, the EITSI, and the Service Providers; Customers are included as appropriate.

All Operational Forums are chaired by the Government and supported by the EITSI.

The initial Operational Governance Forums have been identified as:

- Integrated Services Delivery Forum
  This provides for review and actioning of issues with the full EITS Environment, particularly those issues that cross multiple service providers. This forum provides for participation from all the Integrated Service Providers.
- EITSI Services Forum
  This provides for review and actioning of issues with EITSI Services. The forum reviews service performance metrics, service delivery plans, resource utilization, and provides general management, oversight, and review of the delivery of EITSI Services.
- Service Provider Services Forum
  There will be one of these forums for each Service Provider. Each of these forums provides for review and actioning of issues with that Service Provider Services. The forum reviews service performance metrics, service delivery plans, resource utilization, and provides general management, oversight, and review of the delivery of the Service Provider Services.
- Integration and Collaboration Forum
  This forum provides for discussion of integration and service delivery plans and processes within the EITS Environment. This form has participation from all Integrated Service Providers. This forum does not contend with issues but provides a collaborative space for service provider leadership to acknowledge and work on inter-service provider process areas.

5.2.3 On-Going Programs

The Contractor shall facilitate and coordinate the execution of On-Going Programs within the EITS Environment and the Integrated Services, in compliance with the requirements of the SMM, this PWS, and any Call Orders.

On-Going Programs own the sponsorship and completion of periodic projects that, while not part of day-to-day operations, are critical to accomplish. All operations have some set of recurring projects. These are often monitored by a part of operations and, at the appropriate time they are initiated as a project. The establishment of On-Going Programs is to ensure that the activity is actually initiated and accomplished in the timeframe contemplated (i.e., that the activity is not inappropriately delayed in the face of other operational issues.)

The On-Going Programs are:

Role	Description
SMM Currency	Which provides for the currency of the SMM, ensures that all portions of the SMM are reviewed annually, and as described under section 5.3.2 Continual Improvement and in the SMM.
Technical Currency	Which provides that all assets and software under management are managed to their currency goals, and as described under section 5.4.7.5 Technical Currency, and in the SMM.
Technology Planning	Which provides that the strategic plans for managing technology in the EITS Environment are executed and the plan updated annually, and as described under section 5.3.1.3 IT Technology Planning, and in the SMM.
Cyber Security Planning	Which provides that the Cyber Security Plan for the EITS Environment is executed and updated at least annually, and as described under section 5.3.8 Information Security Management, and in the SMM.
Customer Satisfaction Management	Which provides for the plan and activities to manage customer satisfaction with the Integrated Services, are executed and is updated annually, and as described under 5.6.1 Business Relationship Management, and in the SMM.

The Contractor shall:

- Track On-Going Programs' activity, deliverables, and milestones using the Project Portfolio Management and Reporting system.
- Ensure that the deliverables and plans of the Integrated Service Providers are appropriately tracked according to established SMM processes.

- Monitor On-Going Programs issues and risks and further collaboration to address issues and risks across the Integrated Service Providers and Customer organizations.
- Provide governance of On-Going Programs by establishing forums, meetings, and escalation reports, and ensuring alignment to the EITS Governance as documented in the SMM.
- Establish additional or remove existing On-Going Programs at the direction of the Government.

5.2.4 Operating Level Agreements

The Contractor shall enter into mutually agreed joint governance and issue resolution document(s) with other Integrated Service Providers as Operating Level Agreements (OLA). At a minimum, OLAs will:

- Govern how the Integrated Service Providers coordinate activities, interact and integrate processes, ensure that there are no gaps or unnecessary duplication of responsibility, and will define at an operating level the demarcation of functions and the touch points between such parties
- Describe the key dependencies between the Integrated Service Providers.
- Provide for sharing information, data, technical knowledge, expertise, and resources essential to the implementation of the Integrated Services
- Ensure the greatest degree of cooperation for the delivery of the Integrated Services
- Ensure shared responsibility for achieving required SLAs

The Contractor shall develop, maintain, and adhere to OLAs with the Integrated Service Providers and any other vendors as applicable.

The Contractor shall establish OLAs for any portion of the contract requiring cooperation and coordination with other contractors for delivery of the Integrated Services.

The Contractor shall ensure that all OLAs remain current and consistent with all other relevant documentation (e.g., the SMM, service provider contract, DoD Policies).

Contractor OLAs shall adhere to the requirements in the OLA Outline, in Exhibit 1.2 (Operating Level Agreement Outline).

Each OLA will be subject to the Government's review, comments, and approval. Contractor shall ensure that all other applicable Integrated Service Providers incorporate the Government's comments, resolve any concerns, and obtain the Government's written approval prior to finalization of any such OLA. Similarly, in order for any amendment to an OLA to become effective, such amendment must be approved by the Government.

The Contractor shall establish Operating Level Measures (OLMs), and other supporting measures and controls, for the Integrated Services, as identified in the OLAs and approved by the Government.

The Contractor shall provide a set of actions in the Continual Improvements Register on a quarterly basis to establish and improve OLAs, OLMs, and other supporting measures and controls, for the Integrated Services.

Where OLAs do not exist, Contractor shall proactively work with service providers, Customers, and the Government to deliver to the objectives and overall success of the Integrated Services.

In no event will any term of any OLA established by Contractor reduce, limit, or otherwise adversely affect the provisions of this PWS and any Call Order, or the rights or benefit of the Government or the Customers provided for under this PWS and any Call Order.

5.2.5 Program Management Functions

The Contractor shall support the Government Program Management Office in the management of the portfolio of IT projects and programs within the Integrated Environment, including all IT projects involving DHA and any Customer. Program Management functions include planning, schedule management, cost management, quality management, risk management, and the execution of their programs, projects, or initiatives.

The Program Management Functions manages the portfolio of projects and programs within EITS, including all projects involving the Integrated Service Providers and any Customer. This involvement includes projects elected by a Customer through a Service or Solution Request (e.g., office move), projects initiated as part of other programs, projects initiated by Integrated Service Providers (e.g., stand up a new service, major hardware or software upgrades), projects to onboard a new Service Provider or off-board an existing Service Provider, projects to transition Customers to the Integrated Services, development and maintenance of the integrated SMM, and oversight for On-Going Programs. In addition, the Program Management Function is an important vehicle for communicating with Customers and EITS Governance on activities in the EITS Environment including cross-project resource contention and dependencies.

The Contractor shall align with and account for the standards and processes of the Government Program Management Office, accounting for the required reviews and approvals of these processes.

The Contractor shall direct the project activities within the Project Management practice, including providing project and program management support for cross-service provider projects.

The Contractor shall provide program management support for platform-level projects that impact multiple Customers. Contractor shall provide program management support for individual Customer projects as approved by Government.

The Contractor shall maintain and report to Government and EITS Governance on the portfolio of projects and programs.

5.2.5.1 Project Portfolio Management System

The Project Portfolio Management System is a Service Management System. The Contractor shall manage the enterprise toolset for Project Portfolio Management which provides a common and standard view of all IT projects in the EITS Environment, for the use of DHA, Customers, Integrated Service Providers, and other vendors.

Contractor shall evaluate and recommend priorities for strategic IT service investment proposals, long-term and large-scale, as well as short-term limited-scope opportunities, to

ensure value and adequate return to DHA mission and enterprise, based on the strategic intent and priorities of the mission.

The Contractor shall manage the Project Portfolio Management System as the single source of information regarding all projects for EITS Environment amongst the Integrated Service Providers and designated other vendors. Contractor shall ensure that all project data related to the Integrated Services resides in the system.

The Project Portfolio Management System will at a minimum support the following:

- Provide for the tracking of issues and risks related to a project, program and/or portfolio of projects
- Provide for tracking costs and schedules within and across different projects within the portfolio
- Maintain the relationships between tasks within a project and between projects within the portfolio
- Provide for resource rationalization across different projects, programs, service towers and recipients of services
- Provide for tracking and discovering dependencies across different projects within the portfolio
- Provide a customizable set of views for different stakeholders
- Development of "what if" scenarios to support prioritization

5.2.5.2 In-Process Projects

During the implementation of Service Provider services, the Government and Contractor shall review the list of in-flight projects and in-process work (e.g., requests for services). Government will determine the portion of in-process projects and other in-process work that will become the Service Provider responsibility and a date by which Service Provider shall assume that responsibility.

The Contractor shall ensure that the Service Provider completes all work in accordance with the following:

- DAD IO/J-6 Change management procedures to address any changes in scope, requirements, schedules, or cost in respect to the work.
- DAD IO/J-6 Solution Request and proposal processes in place as of the date the Service Provider is to assume responsibility.
- DAD IO/J-6 Project management and development practices in place as of the date the Service Provider is to assume responsibility for these projects.

5.2.6 Service Management Manual

The Contractor shall develop and maintain the Service Management Manual (SMM) for coordination, management, and reporting of the Integrated Service Providers across the Integrated Environment. The SMM outlines the operational activities designating ITIL 4-based performance standards, processes, and polices for the EITSI interaction with the Service Providers for the delivery of the Integrated Services. The SMM specifies the organization, the tasks, and responsibilities associated with elements in the delivery of the Integrated Services. It contains documentation required, methodologies used, standards,

practices, conventions followed, and details regarding tasks, reviews, and audits conducted to ensure that services meet all contractual requirements.

Contractor shall manage the processes and procedures to support the Integrated Environment, such that the objectives, scope, and principles of the Integrated Environment are achieved. Contractor shall ensure that Service Providers provide all documents and processes that support and describe the scope of the Service Provider services in the SMM.

Contractor shall provide a taxonomy for the organization of the SMM that will accomplish the purpose and goals for the SMM to be the essential repository of all operational knowledge for the EITS Environment. Contractor shall regularly examine and optimize the organization of the SMM to improve the operating environment across all the Integrated Service Providers.

Contractor shall develop the definition and documentation of:

- The policies in the SMM, which set the objectives, scope, and principles that will ensure the success of the Integrated Environment, as provided by the Government
- The processes, sub-processes, and procedures for the Integrated Environment in the SMM, as approved by the Government
- The sub-processes, procedures, and SOPs, for the Integrated Environment to support individual Customers and Customer environments in the SMM, as approved by the Government

Contractor shall verify the effective compliance with the SMM policies, processes, and procedures by the Integrated Service Providers, Customers, and other vendors. Contractor shall provide analysis on such verification at least twice per year. Contractor shall provide an online feedback mechanism to solicit and resolve user comments, corrections, and questions.

Contractor shall secure access to the SMM such that authorized users have appropriate access to the portions that support their function. In particular, the Contractor shall secure the portions of the SMM that pertain to the SIPRNet Environment are only accessible to those authorized users with credentials to work in the SIPRNet Environment.

Contractor shall document issues with the SMM with the service desk as Problems and resolve these issues through the Problem Management practice. Contractor shall manage corrective actions with the Integrated Service Providers and validate required changes with the Government.

In no event will any term or entry in the SMM reduce, limit, or otherwise adversely affect the provisions of this PWS and any Call Order, or the rights or benefit of the Government or the Customers provided for under this PWS and any Call Order.

5.2.6.1 SMM Contents

Contractor shall prove and ensure that each part (e.g., each section, chapter, process, or procedure) of the SMM, at a minimum will provide for:

- Description of purpose and objective
- Other parts and process which interact with this one
- Government policies, rules, regulations, and statutes that apply
- Inputs and triggers

- Reports and other outputs generated
- The specific tasks addressed
- Diagrams for clarity of action and roles
- Operating Level Measures associated
- Identification of roles that interact with this part
    - The responsibilities of those roles
    - Decision and approval authorities within those roles
- Other stakeholders
- Key metrics and measures for performance
- Standard forms, tools, and other work aides
- Revisions and document change controls, history of approvals

Contractor shall provide and ensure that the contents of the Service Management Manual, at a minimum attend to:

- SMM Contents
  The taxonomy and organization of the SMM, the purpose of the SMM, the processes for changing and revising the SMM, governance of the SMM and the process for approving changes, the periods for review and revision of the SMM, and the potential sources of changes to the SMM.
- Organizational Overviews
  This identifies all the organizations that interact through and under the SMM (i.e., Integrated Service Providers, DHA, Customers, Mission Partners). This includes organizational overview descriptions, organization charts, key contacts, key roles and responsibilities.
- Communication
  This provides for the overall Communication Plan that governs the interactions of the Integrated Service Providers with the other participants in the EITS Environment. This identifies specific channels, mechanisms, and media for communication. This provides for procedures for approval and authorization of communications. This designates regular sources for communication messages and processes for emergency and ad hoc communications. This has the historical repository of all communications. This provides for the governance and review of communications.
- Transition
  This provides for the common implementation processes for the transition and implementation of new service provider services in the environment. This provides for interactions with incumbents, the management of implementation schedules and plans, change controls for plans, approval of changes, and facilitating the acceptance of Transition deliverables by the Government. This will include the Integrated Master Schedule of all transition activities for the full implementation of the EITS Environment. This will include the management and tracking of in-process projects and other in-process work that facilitates clean transitions of active work to new Integrated Service Providers.
  Where required this will attend to specific Integrated Service Provider items such as:
    - Transition for the EITSI
      Contains the plan, narrative, and schedule. Contains the deliverables,

acceptance criteria, and timelines. Contains supporting (e.g., knowledge transfer, communications) plans and schedules.
    - Transition for each Service Provider
      Contains the plan, narrative, and schedule. Contains the deliverables, acceptance criteria, and timelines. Contains supporting (e.g., knowledge transfer, communications) plans and schedules.
- Transformation
  Provides for the common processes that support Transformation activities and initiatives, including special projects and other major initiatives being accomplished in the EITS Environment. This provides for interactions with stakeholders, the management of schedules and plans, change control for plans, approval of changes, and facilitating the acceptance of milestones and deliverables by the Government. This will include the Integrated Master Schedule of all transformation and major initiatives across the Integrated Service Providers.
  Where required this will attend to specific Integrated Service Provider Transformation items and activities, such as:
    - For the EITSI
      Contains the plan, narrative, and schedule. Contains the deliverables, acceptance criteria, and timelines. Contains supporting plans and schedules.
    - For each Service Provider
      Contains the plan, narrative, and schedule. Contains the deliverables, acceptance criteria, and timelines. Contains supporting plans and schedules.
    - 4ENO Transition
      This provides for the plans and processes for complying with the 4ENO Transition initiative when the Government chooses to direct that work. At a minimum, contains: Decommission legacy services, ITSM Tools Transfer, Knowledge Transfer, Migration Activities, Post Migration Environment. Cleanup, Test & Validation Activities, Transition Communications, Transition Coordination, Transition Program Management, and Transition SLAs.
- Contract Management
    - EITSI Contract Management processes and practices
    - Service Provider Contract Management processes and practices
- Integrated Environment
    - Integrated Service Provider Management
      This describes the processes, roles, and relationships for the EITSI in facilitating and managing the deliverables of the Integrated Service Providers.
    - EITS Governance
      This describes the governance model and framework; including issue management, roles and responsibilities, definition, purpose, and charters for all operational and relational governance forums, and the library of all meeting minutes, decisions, and actions.
    - On-Going Programs
      This describes the annual cadence of all activities accomplished under the On-Going Programs. This identifies the On-Going Programs, purpose, roles, and stakeholders. This identifies the processes for managing and reporting and decision making around the overall On-Going Programs. This identifies the

roles between the EITSI and the Service Providers for the delivery of On-Going Programs.

- Operating Level Agreements
  This describes the model and interactions between the Integrated Service Providers governed by OLAs. This documents the processes for managing and revising OLAs. This has the library of all OLAs, meetings on OLAs, OLA issues, and OLM achievements.
- Program Management Function
  This provides processes for the management of Programs in support of the DAD IO/J-6. This has all policies and processes for Program Management. This describes the processes for interacting with EITS Governance for decision making for Programs.
- Service Management Manual
  This describes the processes for managing the SMM, including the supporting procedures for document management and control. This also describes the processes for SMM Currency, achieving Single Processes, and improving Process Maturity.
- Service Management Systems
  This describes all the SMS, the governance and ATOs of the SMS. This also provides for analysis and improvement of the SMS. This includes operating and performance characteristics.
- Service Review and Reporting
  This describes processes for service reviews, and processes for reporting, including the Reports Matrix, the Service Levels, and the Operating Level Measures.

- General IT Management Practices
  - Architecture Management practices and processes
  - Continual Improvement practices and processes
  - Strategy Management practices and processes
  - Knowledge Management practices and processes
  - Organizational Change Management practices and processes
  - Service Portfolio Management practices and processes
  - Project Management practices and processes
  - Information Security Management practices and processes
  - Risk Management practices and processes
  - IT Financial Management practices and processes
  - Vendor Management practices and processes
  - Workforce Management practices and processes
- Service Management Practices
  - Availability Management practices and processes
  - Capacity & Perf. Management practices and processes
  - Service Level Management practices and processes
  - Service Continuity Management practices and processes
  - Change Enablement practices and processes
  - Release Management practices and processes
  - IT Asset Management practices and processes
  - Service Configuration Management practices and processes

  - Monitoring & Event Management practices and processes
  - Incident Management practices and processes
  - Problem Management practices and processes
  - Service Request Management practices and processes
  - Service Design practices and processes
  - Service Validation and Testing practices and processes
- Technical Management Practices
  - Deployment Management practices and processes
  - Engineering Management practices and processes
  - Technical Subject Matter Experts practices and processes
- Customer Interfaces Practices
  - Business Relationship Management practices and processes
  - Business Analysis practices and processes
  - Demand Management practices and processes
  - Customer Portal and Reporting practices and processes
  - DHA Global Service Center practices and processes
  - Service Catalog Management practices and processes
- Global Network Operations Practices
  - Circuit Management practices and processes
  - Global Network Operations Center practices and processes
  - Network Performance Monitoring and Management practices and processes
  - DHA SIPRNet Environment Sustainment practices and processes
  - Force Health Protection and Readiness Sustainment practices and processes
- Service Provider Practices
  - For each CSP and GSP
- Customer Processes and other documents
  This provides for the processes specific to Customers, including specific facility procedures and specific Customer credentials.
  - For each type and category of Customer
  - On-board and off-boarding processes for the addition and removal of Customers from the EITS Environment

5.2.6.1 Process Evaluation

The Contractor will administer a process to evaluate all SMM processes on a regular basis, at least annually, and more frequently for processes where targeted process metrics have not been reached. This includes identifying areas where the targeted metrics are not met, and holding regular benchmarks, audits, maturity assessments and reviews. Contractor shall facilitate and coordinate the appropriate involvement of Government and the Integrated Service Providers to review proposed improvements and solicit ongoing feedback.

The Contractor shall maintain an ongoing process improvement plan to address the process improvement opportunities identified. Contractor shall regularly report to the Government and EITS Governance on process evaluation results and the accomplishment of process improvements in the delivery of the Integrated Services.

The Contractor shall conduct an annual audit on the performance of core processes that identifies best practices and opportunities for improvement on all the Integrated Environment

practices. Contractor shall provide reviews of the results and recommendations for addressing findings to EITS Governance.

5.2.6.2 Process Maturity

On an annual basis, Contractor shall produce a plan for maturing processes within the EITS Environment. Contractor shall obtain Government approval of the plan and execute the plan, reporting results on at least a quarterly basis. As part of Contractor's plan, it will assess the maturity of processes using audit checklists against approved SMM documentation and score maturity using industry accepted capability maturity modeling (e.g., Capability Maturity Model Integration).

5.2.6.3 Single Processes

The Contractor shall ensure single processes exist across all operational areas in order to eliminate redundancy and process inefficiency. Contractor shall document where single processes are not followed and track Government approvals for not following single processes.

The Contractor shall produce a quarterly single process compliance assessment and provide for entries in the Continual Improvement Register with action plans and report progress towards closure of Continual Improvement items. Contractor shall base such process improvements on Customer mission outcomes and challenges.

5.2.6.4 SMM Currency

The Contractor shall provide for a program to maintain the SMM and other relevant operational documentation. The SMM Currency is an On-Going Program, for which Contractor shall provide an annual revision and at least quarterly updates.

The Contractor shall provide a maintenance plan for the review and update of all SMM areas (e.g., policies, processes, procedures, work instructions) as approved by Government. Contractor shall facilitate and coordinate the appropriate involvement of Government, Customers, EITS Governance, Service Providers, and other vendors.

As part of SMM Currency, Contractor shall ensure that, at a minimum:

- All Processes have a named owner in accordance with EITS Governance
- All Integrated Environment practices have a named owner within Contractor
- All documents of the SMM (e.g., sub-processes, procedures, working documents, and desk-level instructions) have a named owner within the Contractor and Service Providers
- Government has provided approval to procedures, work instructions and other materials relevant for Customer sites and business units
- All SMM documents are published online in the repository for Government and designated authorized users
- All issues, problems, and customer feedback for the SMM have been considered during the review process

5.2.7 Service Management Systems

The Contractor shall utilize the Government-furnished ITSM system and other Service Management Systems.

The Contractor shall provide an analysis of existing SMS tools to determine if they are efficient and functional as required in Call Orders against this BPA. The Contractor shall provide improvement recommendations to streamline and manage the SMS. The Contractor shall ensure that any proposed hardware or software meets DoD IT security requirements. The Contractor shall ensure that proposed solutions are capable of being hosted in Government Approved Hosting Environment. Government approved recommendations shall be provided to the Continual Improvement practices.

The Contractor shall manage the SMS to a common set of processes and performance standards that will ensure the accomplishment of the goals for the Integrated Environment and DHA's mission, and in accordance to the performance requirements as described in the attachment found in Exhibit 3 (Performance Requirements Summary).

The Contractor shall secure access to all SMS such that authorized users have appropriate access to the tools and functions that support their role. In particular, the Contractor shall secure the portions of the SMS that maintains information on the SIPRNet Environment, such that the information is only accessible to those authorized users with credentials to work in the SIPRNet Environment.

The Contractor shall actively and responsively coordinate deployments of updates to the SMS with the Government and other Government designated contractors.

The Contractor shall conduct/attend walk-throughs and/or meetings where the SMS are discussed, as directed by the Government. The Contractor shall participate in Integrated Product Teams (IPT) as directed by the Government.

5.2.7.1 SMS Tools

Contractor shall utilize the Government provided tools to manage the EITS environment and integrate the Integrated Services. The categories of tools being utilized in the environment, for example:

- IT Service Management (ITSM)
- End-User Support Tool
- Server/Service Monitoring
- Event Management
- Network Infrastructure
- Network Policy Services
- Operating System Management
- Active Directory
- Data At Rest
- IT Service Management
- Log Management
- Security Tools
- User Persona Management
- Wireless Management
- Project and Project Portfolio Management

5.2.7.2 SMS Management

The SMS are managing critical systems as part of a 24x7x365 operations and the business need is for the SMS to be always available to support that mission. The Contractor shall ensure that all SMS for which they are responsible are run in conformance to the defined parameters within their ATO. Where a login is required, the SMS should integrate with the DOD provided token-based authentication, including role-based assignment of access.

The Contractor shall document performance characteristics for the SMS in the SMM, and maintain the SMS to operate within those performance characteristics.

The Contractor shall be responsible to manage the SMS such that:

- Compliance with Government rules and policies, including Government ownership of all data, metadata, business rules and documentation in the SMS
- Provide, make available, and maintain the SMS to meet the objectives for the Integrated Environment for Government, Customers, Service Providers, and designated other vendors
- Provide data models and data dictionaries for all SMS to Government with the ability to extract, transform, and load the information into other data management tools (e.g., a data warehouse)
- Designate performance standards, processes, policies, and other SOPs for the SMS in the SMM
- Maintain the SMS to meet performance standards, processes, and policies requirements, to maximize efficiency, and to minimize outages, as necessary
- Provide for monitoring and event management of the SMS and dependent systems to ensure the availability of the SMS to manage the environment
- Provide access to the SMS to Integrated Service Provider(s), Government, Customers, and authorized other vendors
- Provide for granting additional access in support of other designated third parties (e.g., auditing organizations) upon the request and as directed by Government.
- Integrate the SMS with Service Management Systems of Service Provider(s), Government, Customers, Customer business units and designated other vendors, such that there is:
    - Full integration between SMS of other entities that exist in the environment as of the start of services, and as otherwise specified in Contractor Transition-In plan
    - Plan and execute a Transition-In Plan to transfer legacy SMS data to new systems as specified by Government, ensuring that appropriate historical data is retained
    - Full integration of the supporting databases of the SMS (e.g., CMDB) with the databases of Service Providers, and designated other vendors, as directed by Government
    - Interfaces enabled for integration by Service Providers, Customers, and authorized other vendors, as directed by Government

- Provide Contractor Personnel, Service Provider personnel, Customers, business units of Customers and authorized other vendors with appropriate training in the use of the SMS
- Limit access to each SMS to authorized users designated by the Government and as documented in the SMM
- Partition access to the SMS and supporting databases such that Customers cannot inappropriately access the information of other Customers. Levels of partitioning (e.g., by Customer business unit) will be as directed by Government and documented in the SMM
- Partition Customer information in management and reporting, such that Customers cannot inappropriately access the information of another Customer, as defined by Government
- Provide controls for protecting PII and PHI where it appears in the SMS such that access to such information is fully auditable.
- Support activities to verify the SMS' contents and correctness of the information contained therein by Government, Customers and other designated third parties (e.g., auditing organizations)
- Provide online reporting capability with real time data for use by Government and Customers in the generation of sophisticated, custom reports
- Maintain, update, and implement the SMS archive and backups needed to recover from an outage or corruption within designated timeframes in order to meet Government's requirements, where directed by Government
- Provide physical database management support for the SMS, including providing backups and restores of data within designated timeframes, where directed by Government
- Participate in test and implementation of SMS software and database changes and updates, as directed by Government
- Proactively provide capacity planning for the SMS and prevent situations caused by lack of capacity (e.g., dataset or table space capacity events, full log files).
- Notify Government of situations and risks caused by lack of SMS capacity, and correct those situations as designated by Government
- The SMS provides automated workflow capabilities, where possible
- Maintain separation of duties between system administrator and security personnel
- The Contractor shall produce a set of actions in the Continual Improvements Register for modifications to the systems during and after the Transition-In, and a quarterly release schedule indicating scope, priorities, and schedule performance regarding achieving the improvements

5.2.8 Service Review and Reporting

The Contractor shall provide consolidated service reporting for the Integrated Services using a dashboard that shows current period, prior periods, and data trends and results. Additionally, Contractor shall provide consolidated reporting of SLAs and OLAs for the Integrated Services. The reports are accompanied by Contractor's assessment of risks, issues, lessons learned and opportunities for improvement and includes reporting for the MHS and Mission Partners. Recommendations for improvement that have been approved by the Government will be submitted to Continual Improvement practice.

Service Level reporting and other reporting requirements are set out in Exhibit 3 (Reporting and Service Level Management). The reports are to be accompanied by the Contractor's assessment of risks, issues, and opportunities for improvement, as approved by the Government and EITS Governance.

5.3 General IT Management Practices

The Contractor shall implement and maintain the following general business management practices, as described for ITIL 4 under General Management Practices, and as approved by the Government.

5.3.1 Architecture Management

The Contractor shall implement and manage the practice for Architecture Management across the Integrated Service Providers, as approved by the Government.

The Contractor shall be responsible for application and infrastructure standards by:

- Maintaining, managing, and controlling data, application, and infrastructure architecture standards
- Coordinating activities to evaluate and approve architecture changes
- Processing customer requests
- Reviewing and coordinating approvals for requested changes to standards
- Communicating approved architectures and conducting ongoing research of new infrastructure solutions, techniques, and tools to identify candidates to support current and future mission needs
- Coordinating tool and technology selection efforts, including those resulting from capacity, availability, and service improvement campaigns

5.3.1.1 Standards

The Contractor shall manage and maintain standards for use in the EITS Environment and for support of the Services Catalog, engineering, and Solutions for Service Requests. Contractor shall ensure standards are clearly defined and easily understood by users. Contractor shall work with the Integrated Service Providers to maintain all standard in the Technology Plan.

The Contractor shall track on the use of standards, including Customer expectations, benchmark information (including, but not limited to cost, hours, fulfillment time), and standard fulfillment times. Contractor shall identify trends and multiple uses of alternative products and services such that they become candidates for standard services.

The Contractor shall regularly educate Customers about the need and requirements to use standard services (e.g. bulletins about upgrade requirements, modification of product support, compatibility issues, and known problems with nonstandard products).

The Contractor shall monitor the environment and report the introduction and use of unauthorized products and services within the EITS Environment as specified in the Technology Plan. Contractor shall provide recommendations for remediation or additional standards based on Customer mission needs.

The Contractor shall provide information to Customers who will be affected by the elimination of a standard service at least twelve (12) months prior to the elimination of a standard.

5.3.1.2 Solution Design Management

The Contractor shall provide architectural, engineering, and design support to the Integrated Environment for the delivery of Contractor Services, including Solution Requests and Project Management.

The Contractor shall manage the process for fulfilling requests for technical solution designs and for the capture and validation of solution requirements from Customers. Contractor shall ensure solution designs appropriately addresses total costs, implementation times, and risks. Contractor shall facilitate the approval process of the solution design by Customers and Government.

The Contractor shall monitor and promote adherence to the Technology Plan and approved standards for all Integrated Services. Contractor shall capture and document previous designs for re-use; including, provide recommendation for making solution designs into standard service items and inclusion into the Services Catalog, document, track, and report on each use of a nonstandard design and potential for re-use. Contractor will participate in the exception process for non-standard solution designs, as directed by Government and in compliance with EITS Governance. Contractor shall monitor the use and frequency of non-standard solution designs.

5.3.1.3 IT Technology Planning

Technology Planning will be an On-Going Program. Based on the approved IT Service Strategy, Contractor shall develop and update a proposal for the long-range, comprehensive use of technology within the EITS Environment with consideration given to Customers' information technology systems, processes, technical architecture, and standards as the Technology Plan. Contractor shall produce the Technology Plan in cooperation with the Integrated Service Providers and other vendors as directed by the Government. Contractor shall solicit input from the Government and Customers related to future technology needs and incorporate their input into the Technology Plan. Contractor shall coordinate the aggregation of technical planning information from Government, Customers, Contractor, Service Providers, and other vendors as directed by Customers and in accordance with the SMM.

The Contractor shall ensure that the Technology Plan is developed on an annual basis, and will include a rolling three (3) year projection of anticipated changes, subject to Government mission and planning requirements. Contractor shall provide a quarterly update of the Technology Plan with input from the Integrated Service Providers.

The Contractor shall conduct an annual Technology Planning event based on the results of the Government strategic planning and the approved IT Service Strategy, as a mechanism for gathering input from Customers and key stakeholders on evolving business needs.

As part of the Technology Plan, the Contractor shall propose an approach to implementation with scope, timing, risks, and cost impacts, for Government and Customers. The Contractor

shall propose specific, short-term steps, and potential schedules for projects or changes to occur within the next twelve (12) months.

The Contractor shall ensure that the Technology Plan supports the practice of Service Design. Contractor shall create and regularly update the descriptions of the minimum Equipment and Software requirements and any specific Equipment and Software that are designated for standard use within EITS Environment (e.g. standard services). Contractor shall facilitate and coordinate the update of descriptions from Service Providers and other vendors. Contractor shall publish updates in the Technology Plan on at least a quarterly basis. Contractor shall provide guidance to solution architects and engineers working within Service Design on standards that are within the Technology Plan.

The Contractor shall track and report on new technology advances applicable to the EITS Environment specifying any technical benefits and cost savings that may be achieved by Government or the Customers. Contractor shall facilitate and coordinate the input of the Integrated Service Providers in tracking and reporting on technology advances applicable to the EITS Environment. Contractor shall report on technology advances within and outside of existing Service Providers to Government and Customers on a twice-annual basis.

The Contractor shall identify, evaluate, and track opportunities for efficiency in the delivery of Services that Contractor has observed in the course of delivering the Integrated Services. Contractor shall facilitate and coordinate the input of the Integrated Service Providers in identifying efficiency opportunities. Contractor shall identify and track changes in the Integrated Services that have been made regardless of financial responsibility for underlying assets. Contractor shall review the evaluation of efficiency opportunities with Government and Customers on a twice-annual basis.

The Contractor shall ensure that the Technology Plan supports and aligns to the On-Going Program of Technical Currency:

- Establish and maintain the definitions of Software Currency and Refresh for all Equipment and Software in the EITS Environment in conjunction with Government.
- Establish which software releases and system platforms are not current (i.e. which are approaching end-of-life, which are going out of support, and which have been released and should be considered current)
- Track end-of-life hardware and software to include underlying drivers and firmware resident in the EITS Environment and ensure notification is provided to Government, Customers and Vendors, as documented in the SMM
- Coordinate the remediation of any hardware or software, which have reached end-of-life or are otherwise unsupported
- Contractor shall facilitate and coordinate the update of the definitions of Software Currency and Refresh with the Integrated Service Providers, as approved by the Government
- Contractor shall define Software currency as the most recently released and generally available version of the Software (the “N” release level), unless otherwise directed by Government. Contractor shall define Software currency as release N-1 and earlier versions of the Software as directed by Government or EITS Governance

The Contractor shall publish updates to the definitions of Software Currency and Refresh at least on a twice-annual basis. Contractor shall gather and maintain information on upcoming

Software releases, Software renewals and end-of-support notices to Government and affected Customers. Contractor shall escalate to the Government where changes to the definitions of Software Currency and Refresh will cause financial impacts to the Integrated Services, costs of standard services, costs of standard solutions, the cost of the renewal of retained Software or otherwise result inn changes to costs.

5.3.2 Continual Improvement

Contractor shall conduct improvement planning across the Integrated Services to improve mission aligned IT service quality. Improvement planning will be based upon captured results from the process evaluation, service measurement, and quality assurance programs, as approved by Government.

The Contractor shall establish and conduct the Continual Improvement (CIP) practice. The Contractor shall manage improvements to the Integrated Services and the performance of the Integrated Service Providers by continually measuring, reporting, and coordinating service results. This process will include the establishment and management of a Continual Improvement Registry (CIP Registry) for the execution of CIP functions.

The Contractor shall identify and implement service provision improvements that provide performance or cost benefits to the Government. The Contractor shall elevate ideas for improvements that require Government evaluation and approval through appropriate Government approval authorities. Improvements may include tools, processes, or any other element of this support.

The Contractor shall develop, monitor, and maintain a joint Service Improvement Plan (SIP) across the Integrated Service Providers to manage the delivery of CIP initiatives, as approved by EITS Governance.

The Contractor shall prepare, continuously update, and adhere to a SIP. The SIP shall document how the Contractor will continuously improve performance of Contractor Services. At a minimum, the SIP must outline the procedures that the Contractor will use to foster enhancement of quality, timeliness, responsiveness, customer satisfaction, and demonstrable continuous, quality improvement.

The SIP shall contain a customer satisfaction survey template and customer satisfaction assessment process. The template is subject to Government approval prior to implementation.

The Contractor shall facilitate, on at least a quarterly basis, a review of Continual Improvement and the Service Improvement Plan with all Service Providers and Government within the EITS Governance Structure.

5.3.2.1 Service Measurement and Improvement

The Contractor will provide monitoring and measures for the overall success of delivery of the Integrated Services within the EITS Environment. Opportunities for improvement will be submitted into the CIP Registry and the Continual Improvement practice.

5.3.2.2 Overall Program Measures

The Contractor shall implement and manage Overall Program Measures that describe the overall success of the Integrated Services. The Overall Program Measures shall make evident to MHS stakeholders the viability and efficacy of the entire program of Integrated

Services, and program of Quality of Assurance for ensuring the Integrated Services meet the mission needs of the MHS. Contractor and Government will limit and manage the number of Overall Program Measures to provide focus and broad applicability that reflects the efficacy of the EITS Environment.

The Contractor shall design measures that reflect the overall objectives of the Government for the EITS Environment (e.g. improve service delivery, innovate, and evolve service offerings, ensure cost competitiveness and transparency, protect the efficacy of asset). Contractor shall ensure that measures are comprehensive reflections of the enterprise end-to-end service (e.g. not a single process or program), and that measures reflect multiple levels of activity (e.g. not a single functional area or program). Contractor shall provide for controls and processes that collect information supporting the measures across the Integrated Service Providers and Customers.

The Contractor shall create and execute a reporting plan for Overall Program Measures, that is approved by the Government, which outlines the content, frequency, access, and action items associated with the maintenance of program measures and measurement reports. Contractor shall provide recommendations for adjusting processes, measures, and controls, and recommendations for revising Overall Program Measures at least annually. Contractor shall provide corrective actions and program management to improve the measurement approach and track improvements across the life of the Overall Program Measures.

5.3.3 Strategy Management

The Contractor shall implement and manage the Strategy Management practice across the Integrated Service Providers and other vendors, as directed by the Government. Contractor will develop and manage an integrated IT Service Strategy for the EITS Environment.

Contractor shall provide a process for the establishment, maintenance, tracking, and publication of an IT Service Strategy for the services provided by the Integrated Service Providers that is approved in accordance with EITS Governance. This process exists to set the goals for IT capabilities in support of the DHA's overall IT strategy. Contractor shall provide for an update of the IT Service Strategy at least quarterly.

The IT Service Strategy shall:

- Project future volume, technology, and other changes that could impact Government and Customers systems and technical architectures
- Identify strategies and approaches for future IT delivery that will provide Customers with advantages, increased efficiency, increased performance, or cost savings
- Identify candidates and requirements for the deployment of new technology or services or the automation of tasks associated with the Integrated Services and Customer business processes
- Identify industry and technological trends that may impact Government and Customer plans and services
- Identify and track regulatory issues and changes that may impact the services
- Incorporate data and lessons learned from the operating environment that may impact Government and Customers' plans

Contractor shall perform an assessment of the IT strategy at least annually. Contractor shall analyze the DHA overall IT strategy for the effective use, improvement, and development of

IT services to support the DHA mission, organizational strategy, and enterprise requirements. The Contractor shall incorporate input from the Government, Customers, and Service Providers, and maintain alignment with the EITS Governance processes.

Contractor shall facilitate and encourage active cross-functional, cross-group, and cross-location coordination and communication related to technology or service changes and automation. Contractor shall facilitate appropriate access to specialists within Contractor's broader organization, and the organization of Service Providers, as needed, to assist Government and Customers in developing and updating the plans and standards for the EITS Environment.

5.3.4 Knowledge Management

The Contractor shall establish and manage the practice for Knowledge Management across the Integrated Services to gather, analyze, store, and share knowledge and information within the EITS Environment. The Contractor shall develop and maintain processes for Knowledge Management to improve efficiency and reduce the need to rediscover knowledge.

The Contractor shall develop a library of documentation, which conforms to the documentation standards and format agreed upon by the Government. The Contractor shall develop documentation in accordance with the requirements in the SMM.

The Contractor shall facilitate workflow, process, and tasks to author, publish and ensure all service, operational and other knowledge content is accurate, relevant, protected and most importantly available when and how it is needed. Knowledge material spans all of the Integrated Services and may include technology, resource, component, and service details.

The Contractor shall provide processes and controls to enforce the proper identification of knowledge and information that supports the EITS Environment, such that authorized users can search and find information easily.

The Contractor shall provide for processes and controls for the Integrated Suppliers and other vendors for submitting information into Knowledge Management.

The Contractor shall formulate and deploy a Knowledge Management strategy, to identify relevant service management knowledge, to include the data and information that support this knowledge. This strategy for Knowledge Management shall be developed in consultation with the Government and approved by EITS Governance. Contractor shall formulate a knowledge management taxonomy, which will be approved by Government.

5.3.4.1 Document Data Store System

The Document Data Store is a Service Management System. The Contractor shall manage the Document Data Store to be the single repository for all information on the EITS Environment across all the Integrated Services, including the SMM, training material, FAQs, and similar documentation for Contractor Personnel as well as personnel from Service Providers, other vendors, the Government, Customers, and designated third parties.

The Contractor shall ensure that the tools, processes, and procedures provide for effective data sharing and data profiling across the Integrated Service Providers, other vendors, and Customers business units.

The Contractor shall facilitate integration to the Document Data Store by the Integrated Service Providers and other vendors, as directed by the Government. Contractor shall provide for the ingestion of other knowledge databases and self-help articles from the legacy knowledge management tools.

The Contractor shall provide access to the SMS to authorized users, Service Providers, and other vendors, as directed by the Government.

5.3.4.2 Training

The Contractor shall provide a process for the training of stakeholders on the EITS Environment, including training in SMM processes and SMS tools. The Contractor shall utilize the Government identified training and learning management system.

The Contractor shall provide and maintain training on the Service Management Systems and supporting processes to the Integrated Service Providers, other vendors, and Customers. Contractor shall provide on-going methods for training as tools and processes are updated. Contractor shall ensure that all training is specific to the EITS Environment and applicable to Customers and Service Providers. Contractor shall make training material available online for future reference for those that cannot attend live training, and accessible by all authorized users.

Training may be CBT, conducted virtually, or conducted on-site at DHA supported locations, CONUS, or OCONUS, as required by the Government. Material for training may be presented in a paper or digital media format for computer-based training, tutorials, or other print media.

The Contractor shall provide training on the Integrated Environment (e.g. the purpose, activities, policies, procedures, tools, interfaces) for all stakeholders to ensure effective execution of the process. Contractor shall provide on-going methods for training Contractor Personnel, Service Providers, Customers, and designated other vendors on the Integrated Environment.

The Contractor shall provide and maintain training material for Service Providers (i.e. Contractor Personnel, and personnel from Service Providers and other vendors), that includes at least the following information: the Integrated Services being provided, the value of these Integrated Services to Customers, the financial structure of charges, orientation and summaries on Customers business units, Government policies and rules, orientation to all applicable laws and regulations, the location of document stores, and the structure and location of the SMM. Contractor shall regularly schedule training for these personnel.

The Contractor shall schedule and provide training for authorized users from Customers, on basic IT services based on the needs of Customers. Contractor shall provide training online and, as needed, onsite training. At a minimum, Contractor shall provide training on the main EITS processes, and typical Equipment and Software for end users.

The Contractor shall facilitate the assembly and management of training provided by the Integrated Service Providers on their respective Integrated Services.

The Contractor shall provide a training plan that governs Contractor activities for Training which shall strive to achieve effective training on the Integrated Environment, on a quarterly basis for Government review and approval. As part of the plan, Contractor shall identify

potential training requirements, and recommended training actions to Government and EITS Governance.

Upon request, Contractor shall provide documentation to Customers or designated third parties on the outcomes of training.

The Contractor shall regularly provide guidelines, FAQs, and access to appropriate tools to Service Providers, Customers, and other vendors to promote and reinforce the appropriate use of the Integrated Environment and its supporting policies, processes, sub-processes, and procedures.

5.3.5 Organizational Change Management

In the EITS Environment, the EITSI occupies a key position between Service Providers and Customers and is essential for managing changes that happen between and amongst the participants in that environment. As such, the EITSI is essential for the transition of the Government and Customers to utilizing this new operating model and for sustaining and improving DHA and Customer use of the EITS Environment.

The Contractor shall establish and manage the practice for Organizational Change Management across the Integrated Services to accomplish plan, implement, and manage the smooth and successful implementation of change with the DHA and Customers. The contractor shall facilitate, establish, and distribute the practice of Organizational Change Management within and across the Integrated Environment and the Integrated Service Providers, providing communication, education, and training.

The Contractor shall document its framework and approach to Organizational Change Management, including the industry standard models for organizational change that it will adhere to within the EITS Environment in the SMM. Contractor shall document policies for support and governance of organizational change, as specified by the Government. Contractor shall develop and maintain processes for Organizational Change Management across the Integrated Service Providers and document those in the SMM.

The Contractor shall develop an Organizational Change Management Plan, as described in 5.3.5.1, that will show the activities, schedule, and communications for organizational change in the EITS Environment.

The Contractor shall provide communication and training for all parts of the EITS Environment (e.g. tools it implements and manages, the processes it establishes and manages, and operational governance it facilitates and manages) in support of organizational change. Contractor shall provide regular outreach across multiple channels to those impacted by organizational change and strive to produce a positive posture and relationship for the planned change within those stakeholders.

The Contractor shall conduct regular surveys of those participating in organizational change to gather feedback on the process and outcomes. Contractor shall analyze the survey results and provide recommendations to the Government for adjustments to plans.

The Contractor shall provide an analysis on the effectiveness of Organizational Change Management which will include objective and subjective measures of the shortcomings of organizational change (e.g. the volume of end user calls that could have been prevented with improved training and awareness, the tenor of comments and complaints to the Business

Relationship Management and EITS Governance, the adherence of activities to planned timelines, the health of relationships between stakeholders, the tangible measures of support from DHA leadership).

5.3.5.1 Organizational Change Management Plan

The Contractor shall develop and maintain a continuous Organizational Change Management Plan which will comprise the schedule and activities to accomplish the goals for Organizational Change Management within the EITS Environment and coordinates the activities of the Integrated Service Providers, the Government, Customers, and other vendors.

The Contractor shall provide an annual revision of the Organizational Change Management Plan and at least quarterly updates, as approved by Government. Contractor shall facilitate and coordinate the appropriate involvement of Government, Customers, EITS Governance, Service Providers, and other vendors.

The Organizational Change Management Plan will include a communications plan that identifies the mechanisms and channels for communication and identifies key messages that need to be address along the schedule of change. This will identify the different stakeholders for receipt and creation of communications across DHA and Customers. Contractor shall regularly track and gather information on communications activities and the effectiveness of organizational change communications.

The Organizational Change Management Plan will encompass results from Business Relationship Management and the business analysis of the Customers. Revisions of the plan will address Customers' satisfaction surveys and results from organizational change feedback surveys.

The Contractor shall track execution against the plan, including progress against the projected schedule and provide recommendations for adjustments to the plan.

5.3.6 Service Portfolio Management

The Contractor shall coordinate Service Portfolio Management ensuring that Customers have an optimum mix of services to meet required mission outcomes. The Contractor shall assist Customers in proactive management across the service life cycle, including those services in the concept, design, and transition phases, as well as live services defined in the service catalog and those services that are retired or being sunset.

The Contractor shall conduct and maintain an inventory of the operational services (e.g. those in the Service Catalog), proposed services (service pipeline), and decommissioned services (retired services). Contractor shall maintain the services in a Service Portfolio database system for access by authorized users and the Government. Contractor shall manage and track all Service Portfolio updates, additions or other changes, in accordance with the SMM. Contractor shall integrate reviews and approvals required in from the Government for the management of the life cycle of services. Contractor shall ensure that all service in the service portfolio include a standard and minimum set of attributes as defined in the SMM. Contractor shall ensure that the Service Catalog and Service Portfolio systems are accurate and current in accordance with the SMM.

The Contractor shall gather and coordinate on potential improvements to the portfolio of services as identified by the Integrated Service Providers. Contractor shall periodically

provide analysis of the service portfolio to determine whether the services still meet their objectives and if they are still appropriate for the strategy as documented in the Technology Plan. Contractor shall document the basis and frequency of such analysis in the SMM. Contractor shall regularly identify and validate all proposed new services and existing services and provide recommendations to the Government on changes to the portfolio of services. Contractor shall survey Customers concerning potential improvements and existing deficits.

The Contractor shall work with Service Providers to respond to Government and Customer requests for new services or significant changes to existing services. Contractor shall provide proposals for requested new or changed services within timeframes identified in the SMM. Contractor shall provide mechanisms, processes, and procedures to capture feedback and mission needs from Customers as to change in Services.

The Contractor shall work with prospective new Service Providers to plan, develop, and onboard new services to be part of the Integrated Services.

5.3.6.1 Service Portfolio Management System

The Service Portfolio Management System is a Service Management System. The Contractor shall manage the enterprise toolset for Service Portfolio Management which provides a common and standard view of all services in the EITS Environment and the life cycle of those services, for the use of DHA, Customers, Integrated Service Providers, and other vendors. Contractor shall ensure that the Service Portfolio Management System provides a database of all Integrated Services including those under development, in operations, or in process of retirement.

5.3.7 Project Management

The Contractor shall implement and manage the practice for Project Management across the Integrated Service Providers, as approved by the Government. Contractor shall utilize the Government identified SMS in Project Portfolio Management System to accomplish these project management activities.

The Contractor shall plan and coordinate the Integrated Service Provider resources to implement a major deployment or release (project) within the predicted cost, time, and quality estimates; and to ensure that issues and risks that inhibit success are managed. The Contractor shall align projects to requirements and deliver projects from request through to end solution including turnover to customers and validation that project requirements were met in terms of timing, quality, cost, and execution.

The Contractor shall ensure that all projects are managing risks, changes, issues, communications, and schedules in compliance with the policies, processes, and procedures documented in the SMM. Contractor shall initiate appropriate escalation of project issues and risks to the designated management within the Integrated Service Providers and Customers. Contractor shall ensure all projects are following a standard process for establishing project baselines as approved by Customers.

The Contractor shall coordinate project tracking efforts and communications between all parties until project completion. Contractor shall retain overall responsibility and ownership

of projects until project completion is accepted by Customers. Contractor shall provide scope and cost controls to ensure projects deliver to projected costs and timelines.

The Contractor shall provide for processes and controls to support change in projects that protect the project objectives and the value expected by the Government and Customer. Contractor shall ensure that every project change has an appropriate sign-off from the authorized Customer.

The Contractor shall ensure all projects have a fully qualified and named project manager from the Integrated Service Provider who owns the success of the execution of the project. Contractor shall provide Project Management for all cross-domain projects or programs. Contractor shall manage an integrated project plan where there are multiple projects or cross-domain services.

The Contractor shall develop and utilize common tools, templates, and procedures to enhance the successful completion of projects. Contractor shall ensure those common tools, templates and procedures are made available and communicated to the Integrated Service Providers and Customers. Contractor shall provide a base set of project templates for common projects executed in the EITS environment.

The Contractor shall conduct regularly scheduled Project Management meetings with all Integrated Service Providers to ensure the successful completion of all projects. Contractor shall establish a single focal point for project considerations and issues in order to minimize the probability of conflicting priorities. Contractor shall track the success of projects against such factors as time-commitments, resource utilization, scope, and costs. Contractor shall regularly review projects to identify reoccurring problem areas and make recommendations to the Government for the resolution of those areas. Contractor shall submit Government approved recommendations to the Continual Improvement practice.

5.3.7.1 Project Planning

The Contractor shall coordinate the preparation of proposals and plans for projects as requested by Customers or as appropriate based on providing the Integrated Services. Such proposals and plans will be provided to Customers in a consistent structure and format. Contractor shall coordinate proposal creation with the Integrated Service Providers and other vendors, and in conjunction with the Request for Solution processes.

When the Government approves a project related to the Integrated Services, Contractor shall ensure that a project manager is assigned to the project from the Integrated Service Providers. Contractor shall establish and track project success against a baseline of scope, time, resources, and cost. After the Customer approves the acceptance and completion of a project, Contractor shall provide for project close-out, including performance against baseline, and post-mortem reporting.

5.3.8 Information Security Management

The practice for Information Security Management under the DAD/IO J-6 currently belongs to and is conducted by the DHA Cyber Security Division (CSD). The Contractor shall support and augment this practice for Information Security Management across the Integrated Service Providers, as directed by the Government.

The Contractor shall develop, implement, and maintain internal standards, objectives, processes, and procedures to maintain compliance with Government policies and rules, and Customer requirements.

The Contractor shall ensure the Confidentiality, Integrity, and Availability (CIA) of the Government's information, data, and IT services. The Contractor shall assess that all security risks associated with the delivery of Integrated Services are appropriately identified, evaluated, and appropriate controls are implemented and maintained.

The Contractor shall identify as risks those core items whose failure could lead to a breach of Information System security. Contractor shall elevate identified security risks to EITS Governance and the DHA Authorizing Official for acceptance, mitigation, or other actions.

The Contractor shall follow the Government defined Risk Management Framework (RMF) for accrediting Information Systems.

For each Information System, the Contractor shall facilitate and coordinate the Integrated Service Providers in developing a security assurance strategy to ensure that the requirements, design, implementation, and operating procedures for the identified product minimize or eliminate the potential for breaches of Information System security, and obtain approval from the designated system owner (e.g. Customer) of those strategies. Contractor shall maintain and sustain compliance with all commercial security patches including applicable Security Technical Implementation Guide (STIG) and Information Assurance (Cybersecurity) Vulnerability Alert (IAVA) messages for Integrated Service Providers managed Information Systems, applications, and tools.

The Contractor shall ensure that all Information Systems managed by the Integrated Service Providers are continuously accredited in accordance with RMF requirements, the publications, and subsequent publications and regulations. The Contractor shall proactively identify proposed or pending changes to Integrated Service Provider managed Information Systems that would be considered "major changes" for RMF certification purposes and perform risk mitigation activities.

The Contractor shall register and subscribe to United States CERT and vendor websites to be alerted to all released security advisories, security alerts, updates, and work-around. The Contractor shall coordinate with all application owners and Tier 3 vendors to ensure compliance with all commercial vendor-released security patches for Integrated Service Providers managed Information Systems, applications, and tools.

The Contractor shall record the strategy in the Cyber Security Plan and upon receipt of government concurrence, implement the strategy, and produce evidence, as part of required software products, that the security assurance strategy has been carried out.

The Contractor shall protect against unauthorized disclosure of data to protect the privacy of Government contractors and private individuals on which the information is maintained. Contractor shall maintain adequate controls and protection of sensitive data to meet DoD and DHA policies.

The Contractor shall ensure that deployed applications meet the features of Identification and Authentication, Auditing, and Discretionary Access Control. Additionally, the contractor will employ compliant encryption in accordance with DoD and DHA policies, and digital certificates for web-based components.

The Contractor shall implement and maintain a security awareness program to ensure that Integrated Service Provider personnel are aware of Government policies and rules, and the security and operational requirements of the EITS Environment and Integrated Environment.

The Contractor shall track the status of any remediation efforts as defined in any outstanding Plans of Actions and Milestones.

5.3.8.1 Cybersecurity Vulnerability Scans

The Contractor shall provide support to assess information assurance and cybersecurity vulnerabilities in the infrastructure and applications operated in the EITS Environment. The Contractor shall ensure that all Information Systems, applications, and tools that reside in a .mil domain and managed by Integrated Service Providers are scanned on a monthly basis or as requested by the Government.

The Contractor shall utilize the Government directed Vulnerability Management System (i.e. Information Assurance (cybersecurity) tools) to provide compliance and scanning and submit scans to eMASS to provide compliance scoring in compliance with RMF. (Currently this tool is ACAS, Defense Information Systems Agency (DISA) Gold Disk Security Readiness Review or the DISA Unix Security Readiness Review depending on the operating system installed on the device).

The Contractor shall submit a copy of the scan results to DHA Cyber Security Division on a monthly basis or as requested by the Government. The Contractor shall report compliance for the infrastructure and applications via the designated DoD Vulnerability Management System, or as directed by the Government.

5.3.8.2 Cyber Security Planning

The Contractor shall develop and maintain a continuous Cyber Security Plan that complies with Government policies and rules, which will comprise the on-going activities that accomplish the goals for Cyber Security Management and coordinates the activities of the Integrated Service Providers, the Government, Customers, and other vendors as identified by the Government. Cyber Security Planning will be an On-Going Program, for which the Contractor shall provide an annual revision of the Cyber Security Plan and at least quarterly updates.

The Contractor shall ensure that the Cyber Security Plan comprehensively defines the cybersecurity requirements of the EITS Environment and supports the security of the Government information technology systems, Equipment, Software, and information. The Cyber Security Plan will govern the periodic activities for security operations conducted by the Contractor and other Service Providers including periodic patching, plans for implementing security measures, security performance monitoring, and periodic security assessments and testing, as defined in the SMM.

The Contractor shall document and maintain the comprehensive security policy that defines the security requirements of the EITS Environment and supports the security of the Government systems, Equipment, Software, and information, within the Cyber Security Plan.

Contractor shall gain approval of the Cyber Security Plan from the EITS Governance and the DHA CSD. Contractor shall provide monthly reviews of progress against the Cyber Security Plan with DHA CSD.

5.3.9 Risk Management

The Contractor shall implement and manage a practice for Risk Management across the Integrated Service Providers, as approved by the Government that augments and supports Government practices for Risk Management.

The Contractor is charged with providing Risk Management related to the EITS Environment and Integrated Services within the context of the overall business risks. The goal of this Risk Management is to identify, assess, and control risks. This includes quantifying the impact to the business that a loss of service or asset would have, and then to manage the activity to mitigate the identified risks across the Integrated Service Providers.

The Contractor shall provide processes that support and adhere to the framework for risk management provided by the Government across the Integrated Services. Contractor shall document and maintain sections of the SMM to include the Government policies and rules, processes, tools, and standards as to Risk Management.

The Contractor shall coordinate initial Service Provider implementations and ensure continual maintenance of standard tools and processes for risk management. Contractor shall incorporate coverage of the interactions between Integrated Service Providers to support the effective design and operation of key controls, and the monitoring and reporting of risk. Contractor shall implement risk indicators across the Integrated Services to monitor risk and assist in the detection of emerging trends and control failures. Contractor shall coordinate Risk Management activities with the practice for Monitoring and Event Management to detect risks and emerging trends.

The Contractor shall assess and recommend improvements based on security vulnerability and risk assessments. Upon direction of the Government, Contractor shall create a Plan of Actions and Milestones detailing the plan to remediate or mitigate risks within the timeframe established by Government or the Customer.

The Contractor shall monitor Service Providers delivery and reporting on the effectiveness of key controls to ensure compliance with Risk Management and Government policies. Contractor shall conduct formal monthly meetings with each Integrated Service Provider to review their progress in addressing risks that need to be mitigated in their services.

The Contractor shall support the appropriate EITS Governance forums with specific risk content as defined by Government.

The Contractor shall operate a quarterly forum with all the Integrated Service Providers and EITS Governance and other Government designated entities. At this forum, Contractor shall review progress in addressing identified risks to be mitigated in the end-to-end delivery of services. As well, Contractor shall review emerging trends and risks, and the effectiveness of key controls.

5.3.10 IT Financial Management

The Contractor shall assist the Government in the evaluation of Financial Management of IT services. The Contractor shall recommend and use models which include cost-effective stewardship of the IT assets and the financial resources used in providing the Integrated Services, enabling the dissemination of information to support critical decisions and activities. It provides quantification, in financial terms, of the value of IT services, the value

of the assets underlying the provisioning of those services, and the qualification of operational forecasting to individual customers and the MHS.

5.3.11 Vendor Management

The Contractor shall assist with the implementation and management of a practice for Vendor Management, as approved by the Government that augments and supports the Government practices for Vendor Management. Contractor shall cooperate and collaborate with these other vendors being managed by the Government. Contracts with these other vendors will be established and owned by the Government. The other vendors will be identified by the Government as required.

The Contractor shall work to integrate other vendor services into the EITS Environment to support the requirements of the Integrated Environment.

The Contractor shall seek to manage and coordinate the activities of the other vendors in accordance with the SMM and Government policies and rules. Contractor shall monitor and report on the adherence of other vendors to the processes in the SMM.

5.3.12 Workforce Management

The Contractor shall implement and manage a practice for Workforce Management, as approved by the Government that augments and supports the Government practices. Contractor shall establish processes for Workforce Management for managing and tracking certain personnel from Integrated Service Providers and other vendors.

The Contractor shall provide an integrated set of processes that will track and optimize the use of specific categories of staff labor and work to improve their productivity. The Contractor shall effectively plan staff schedules and forecast labor requirements. Contractor shall strive to meet the standards for service quality while controlling any associated costs to be within projected boundaries.

5.4 Service Management Practices

The Contractor shall implement and maintain the following service management practices, as described for ITIL 4 under Service Management Practices, and as approved by the Government.

5.4.1 Availability Management

The Contractor shall implement and manage the Availability Management practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall ensure that the level of service availability delivered in all Integrated Services is matched to, or exceeds, the current and future needs of the mission, in a cost-effective manner. The Contractor shall define, analyze, plan, measure and improve all aspects of the availability of the Integrated Services. Contractor shall provide a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets are established, measured, and achieved.

The Contractor shall regularly review the Government provided mission essential functions, and the availability, reliability, maintainability, and recovery requirements for each of those mission essential functions across the Integrated Service Providers. Contractor shall

collaborate and facilitate the Integrated Service Providers to provide a comprehensive view on availability and provide recommendations to the Government for improving availability. Contractor shall provide the Government approved recommendations into Continual Improvement for implementation.

The Contractor shall create an annual Availability Plan to support the services offered in the EITS Environment with the Integrated Service Providers. Contractor shall facilitate and coordinate the Integrated Service Providers in executing the Availability Plan. The Availability Plan shall provide for:

- How availability is improved
- How availability aligns to mission needs
- How availability is improved for unplanned outages, planned outages, and maintenance
- How availability is tracked, monitored, and reported

The Contractor shall coordinate, collate, and consolidated information on all key elements of availability for all the Integrated Service Providers (including impact assessments, outage reports, service level attainment, and analysis of trends). Such information will include current and historical availability metrics and a 12-month rolling forecast. Contractor will retain at least 36 months of availability source data for all the Integrated Service Providers. Contractor shall provide recommendations for Availability reporting and develop measures in cooperation with the Government. The monthly availability report should include elements such as:

- Mean time between failures
- Service Availability and Unavailability
- Major Availability incidents (including impact)
- Service Outage Reports
- Planned versus actual downtime
- Customer complaints and compliments
- Audit, Incident, and Problem reports

The Contractor shall track, monitor, and coordinate investigations of end to end performance of IT services and systems for each defined business function. Contractor shall provide analysis and reporting on a monthly basis, to include:

- Evolving business availability requirements with Customers
- Component failure impact analysis and identify single points of failure
- Mitigation strategies to reduce the likelihood of availability incidents and events
- Recommendations for additional infrastructure and resources (including cost estimates) to mitigate availability risks

5.4.2 Capacity and Performance Management

The Contractor shall implement and manage the Capacity and Performance Management practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall assess mission requirements, operations, IT infrastructure, and will ensure that capacity in the EITS Environment is matched to the current and future needs of the mission. The Contractor shall strive to ensure that the capacity of IT services

and the IT infrastructure is able to deliver the agreed service level targets in a cost effective and timely manner.

The Contractor shall implement, manage, and maintain Capacity Management processes across the Integrated Service Providers. Contractor shall establish a standard approach to utilizing capacity management tools and ensure that Integrated Service Providers consolidate capacity management functions and information into the integrated Capacity Management tool.

The Contractor shall collect and collate system utilization data and other capacity reports from the Integrated Service Providers and other vendors as directed by the Government. Contractor shall identify and track capacity trends, issues, and risks.

The Contractor shall develop and plan the overall Capacity Management strategy for the Integrated Services. Contractor shall communicate and coordinate with Government and Customers to understand future mission needs and requirements. Contractor shall forecast future capacity needs based upon communicated mission needs and system utilization data. Contractor shall identify initiatives that impact future capacity levels and suggest actions to align mission needs with future capacity.

The Contractor shall communicate Customer demand forecasts to the Integrated Service Providers. Contractor shall ensure that the Integrated Service Providers formally review capacity requirements for their services. Contractor shall review Customer requests (e.g. in Service Request Management, Service Desk, Business Relationship Management) to identify gaps in service and deployed capacity. Contractor shall identify any service and capacity gaps to the Government as they are identified.

The Contractor shall conduct quarterly reviews and analysis of the capacity supporting the Integrated Services. Contractor shall report on capacity to the Government, identifying capacity problems and making recommendations. Contractor shall initiate Problem Management as appropriate to address potential capacity issues and risks. Contractor shall provide recommendations as approved by the Government to the Continual Improvement practice.

The Contractor shall coordinate the creation of an annual Integrated Capacity Plan for the EITS Environment, including individual Service Provider capacity plans, which reflect the current and future needs of the mission. Contractor shall maintain and provide updates to Integrated Capacity Plan on at least a quarterly basis, unless otherwise specified by Government. Contractor shall incorporate Customer plans for capacity and other mission needs in the Integrated Capacity Plan. The Integrated Capacity Plan will include, at a minimum: goals, objectives, scope, and methods; comparisons to baseline; current levels of resource utilization; current levels of availability; current levels of service performance; forecasts for future requirements; and assumptions and recommendations.

5.4.2.1 Capacity Management System

The Capacity Management System is a Service Management System. The Contractor shall manage and operate the Capacity Management System across all the Integrated Services. Contractor shall implement and maintain the SMS that will serve as the single source of information regarding capacity for the Integrated Services. Contractor shall ensure that all information necessary for managing, forecasting, and reporting on capacity is required and

maintained in the SMS, as identified in the SMM. Contractor shall utilize the SMS for the compilation, collation, maintenance and publishing of capacity measures and forecasts for all Integrated Service Providers and other vendors, as directed by the Government.

5.4.3 Service Level Management

The Contractor shall maintain, monitor, and report on service quality through a continual review of IT service achievements based upon SLAs and OLAs. Service Level Management establishes SLAs with the Government and OLAs between Service Providers ensuring that all services are appropriate, and to monitor and report on service quality and achievement. Service Level reporting and other reporting requirements are set out in Exhibit 3 (Reporting and Service Level Management). The reports shall be accompanied by the Contractor's assessment of risks, issues, and opportunities for improvement, as approved by the Government and EITS Governance.

The Contractor shall implement, monitor, and maintain processes and tools that enable consistent delivery of Service Level Management across the Integrated Services, in accordance with Exhibit 3 (Reporting and Service Level Management). Contractor shall require and coordinate the Integrated Service Providers use of such processes and tools.

The Contractor shall provide for regular reoccurring Service Level Management activities and governance. Contractor shall define triggers for event driven Service Level Management activities to be included in the SMM.

On a schedule agreed upon with Government and as documented in the SMM, Contractor shall monitor and measure end-to-end services against targets in the Service Levels and coordinate actions to eradicate unacceptable levels of service across all Integrated Service Providers.

On a quarterly basis, the Contractor shall conduct end-to-end service reviews with representatives of each Integrated Service Provider to assess required measurements and service improvement plans. Contractor shall analyze customer satisfaction across the entire customer experience and assess service improvement plans. Contractor shall provide proposals for service improvement, and provide Government approved plans to the Continual Improvement practice for implementation.

The Contractor shall collect, track, and maintain performance on additional Operating Level Measures (OLM) established with Customers and Mission Partners, as directed by the Government.

Contractor shall collect and collate supporting source data relating to the Service Levels from all Integrated Service Providers and use such data to produce the service reports.

5.4.3.1 Service Level Management and Reporting System

The Service Level Management and Reporting System is a Service Management System. The Contractor shall manage and operate the Service Level Management and Reporting System across all the Integrated Services.

The Contractor shall implement and maintain the SMS that will serve as the single source of information regarding Service Levels for the Integrated Services. Contractor shall ensure that all information necessary for managing and reporting Service Levels is required and

maintained in the SMS, as identified in the SMM. Contractor shall utilize the SMS for the compilation, collation, maintenance, and publishing of service level measures and operating level measures for all Integrated Service Providers and other vendors, as directed by the Government. Contractor shall ensure the SMS will at a minimum:

- Provide for the support of existing Service Level Reporting from legacy systems
- Provide ability to view Service Levels by enterprise and Customer
- Provide ability to view source data and measures that accumulate into each service level measure
- Provide dashboard for view of Service Levels status in near real time

Contractor shall provide for logging of all modifications to the SMS, to provide full tracking, audit trail, and change control at the named-user level.

5.4.4 Service Continuity Management

The Contractor shall implement and manage the Service Continuity Management practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall ensure that systems are operated in accordance with required service levels by:

- Reducing the risk from threat events (e.g. natural/environment, human/man-made, utility – power/network, supply chain, equipment, facility, and loss of key personnel) to an acceptable level and planning for the recovery of IT services
- Designing services to support Business Continuity Management
- Coordinating with Service Providers for a Program of Disaster Recovery preparedness that supports overall Business Continuity and Disaster Recovery processes
- Providing plans that support the rapid and orderly restoral of IT services

5.4.5 Change Enablement

The Contractor shall implement and manage the Change Enablement practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall coordinate change control and configuration management through an end-to-end process to minimize risk, cost, and business disruption, while protecting the computing and delivery of the Integrated Services.

The Contractor shall implement a standardized, integrated Change Management process and supporting procedures for the efficient and effective handling of all changes to the Integrated Services, including the operation of Change Advisory Boards to oversee and assist with operational Changes, that are subject to approval from the Government and EITS Governance, in a way that minimizes risk exposure and maximizes availability of the Integrated Services. Contractor shall establish a standard approach to utilizing change management tools and ensure that the Integrated Service Providers participate and conform to the Change Management processes.

The Contractor shall document all Change Management activity in accordance with the requirements in the SMM and communicate such process and procedures to the Integrated Service Providers and other vendors as directed by the Government.

The Contractor shall assist the Government to define the criteria for normal Changes, Emergency Changes, and Standard Changes, and document that criteria in the SMM. Contractor shall ensure clear definition for Standard Changes that can be actioned through the Service Request process. Contractor shall provide for the capability to pre-approve Standard Changes, and document such approvals in the SMM. Contractor shall provide a process for unscheduled maintenance and non-standard changes.

The Contractor shall facilitate and coordinate information exchanges between and among the Service Providers in order to drive an effective integrated Change Management process. Contractor shall coordinate Change Management activities across all functions, sites, regions, Service Providers, and other vendors that provide services in the EITS Environment.

The Contractor shall facilitate and coordinate all Change Management meetings in accordance with the SMM. Contractor shall run the Change Advisory Board (CAB) to verify the effective execution of Change Management and that an appropriate review of planned Operational Changes takes place with due consideration of the mission and technology risk of planned Operational Changes.

The Contractor shall coordinate the submission of proposed Operational Changes to Customers, in advance of Change Management meetings. The Contractor shall provide for the review of the CI's related to the Change and the operational documentation for specific notes on change procedures. The Contractor shall review proposed Changes and schedules with Customers and the Service Providers to coordinate and obtain all necessary approvals for proposed Operational Changes.

The Contractor shall coordinate with all potentially affected parties by the Change to minimize disruption of normal business operation (e.g. Customers, Service Providers, other vendors, third parties, and designated representatives at sites).

The Contractor shall provide an audit trail of all Operational Changes, including a record of the Operational Change made and the authorization to make the Operational Change. Contractor shall provide evidence that the Integrated Service Providers create accurate and complete records detailing the life cycle of every individual Change for every request for Change received (even those that are subsequently rejected).

The Contractor shall create and maintain a log of all scheduled upcoming Releases and Operational Changes as part of the Change Management process. Contractor shall provide a calendar of expected future Release and Operational Changes to Customers projecting out for at least the next ninety (90) days and renewed on a weekly basis. Contractor shall document regular periods for scheduled maintenance, standard changes, and emergency changes. Contractor shall provide mechanisms for Customers to request custom freeze periods based on their mission requirements. Contractor shall develop schedules in conformance with defined freezes and Maintenance Periods.

The Contractor shall regularly provide analysis and recommendations for evolving the Change Schedule to include all portions of the IT enterprise.

The Contractor shall create rollout, test, and roll back plans for every request for an Operational Change to the Services. Contractor shall coordinate activity across all Integrated Service Providers to update operational and other documentation affected by an Operational Change. Where successful Changes result in an Incident because of that Change, Contractor will consider executing the roll back plan against the Change, as approved by Customers.

The Contractor shall conduct post implementation reviews, per the practice for Change Enablement under ITIL 4, across all Integrated Service Provider for Operational Changes to determine if the Operational Change was successful and to identify opportunities for improvement. Such reviews will include whether or not the change was completed on the first attempt, and a measure of any disruption associated with the change.

5.4.5.1 Change Management System

The Change Management System is a Service Management System. The Contractor shall manage and operate the Change Management System across the EITS Environment, to include all Integrated Service Providers other vendors as designated by the Government.

The Contractor shall develop and implement a standardized method and procedure for the efficient and effective handling of all Changes within the SMS, including the CABs ability to manage Changes. Contractor shall provide processes to utilize the SMS to automate the recording, assessing, scheduling, documenting, tracking, and reporting on Changes to the environment.

The Contractor shall integrate the Change Management System to the IT Asset and Configuration Management System (and CMDB).

The Contractor shall provide for the logging of all modifications to Change records in the SMS, to provide full tracking, audit trail, and change control at the named-user level.

The Contractor shall provide processes and utilize the SMS to describe and effect the communication plans associated with Changes.

5.4.5.2 Change Evaluation

The Contractor shall implement, maintain, and operate a common Change Evaluation process across the EITS Environment, and document the process in the SMM. Contractor shall facilitate and coordinate the Change Evaluation process across all Service Providers.

The Contractor shall establish the policy for when to apply Change Evaluation to the Integrated Services, as approved by the Government. Contractor shall ensure that Change Evaluation is appropriately applied by the Integrated Service Providers.

The Contractor shall facilitate the planning of the Change Evaluation based on formal design packages. Contractor shall evaluate the predicted performance to analyze the intended and unintended effects of a Change. Contractor shall assess risk based on the required specifications, predicted performance, and the acceptance criteria for the proposed Change. Contractor shall coordinate the assessment of cyber security risks with the Government. Contractor shall provide the results of the evaluation to the Government.

After implementation of a Change, Contractor shall gather input from the Integrated Service Providers and Customers regarding actual performance of the Service. Contractor shall compile all findings in a Change Evaluation Report, which will inform the post implementation review carried out by Change Enablement.

5.4.6 Release Management

The Contractor shall provide and manage the practice for Release Management within the EITS Environment. Contractor shall document the guidelines for utilizing Release

Management in the SMM. At a minimum, Contractor shall designate major Changes (e.g. the introduction of a new service, a substantial change to an existing service, and large numbers of related and dependent Changes) as a Release.

The Contractor shall assess the risk to the operating environment for all Releases, and gain Government approval before Changes are allowed to proceed. Contractor shall implement and monitor adherence to the controls for risk management and to achieve compliance with Government policies and regulations, Customer policies, and other standards as documented in the SMM.

The Contractor shall automate and facilitate workflows, processes, evaluation, and reporting, for Release and deployment activities to control and mitigate risk to the operational environment. Contractor shall provide processes for planning, scheduling, and controlling the movement of Releases through the service life cycle.

The Contractor shall assign an EITSI staff person to act as the single point of contact for each Release.

The Contractor shall facilitate and coordinate the Integrated Service Providers in developing implementation and back-out plans for approved Changes that will be included in Releases. That planning shall include the build, track, and coordination of the testing and implementation, and, if necessary, back-out of all Changes. Contractor shall produce impact assessments in support of Release planning. Contractor shall coordinate the resolution of Release issues across the Integrated Service Providers.

The Contractor shall develop and coordinate Release communications, preparations, and training activities, in coordination with the Integrated Service Providers, Customers, and the Government.

The Contractor shall establish and manage the provision of a burn-in period from the Service Providers for a period of time directly after the deployment of a Release, which shall include a review of the key performance indicators, Service Levels, monitoring thresholds, and the provision of additional resources for Incident and Problem Management.

5.4.7 IT Asset Management

The Contractor shall implement and manage an IT Asset Management practice to manage the entire life cycle of all the IT Assets in the ETIS environment. The Contractor shall implement processes that maximizes the value of assets, controls costs, manages risks, enables decision making, tracks asset utilization, and facilitates the appropriate retirement decommissioning of assets in the EITS environment. The Contractor shall obtain and maintain asset and configuration information about all IT assets. Contractor shall maintain and update information to ensure that it reflect the actual state of the IT infrastructure. The Contractor shall manage and maintain traceability of all aspects of each asset and configuration, including identification, planning, change control and management, release management and maintenance.

The Contractor shall provide processes, documented in the SMM, to maintain asset inventory and configuration information for all Integrated Services and managed assets, such that:

- Ensure that asset management processes are followed

- Enables Contractor and Service Providers to record, the individual data elements for each asset as part of the inventory
- Ensure CIs are current and accurate following any change (e.g. modification, addition, or decommission)
- Enables Government and Customers approval of the asset inventory and changes to the asset inventory
- Provides for controls, processes and notifications that support Government and the Customers ability to approve and submit corrections to the asset inventory
- Track and manage all purchased Equipment for the EITSI Environment
- Receive assets and coordinate with Government to ensure delivery to correct locations
- Track managed assets by owner and location
- Facilitate the disposal of assets in accordance with DoD asset policies and regulations

The Contractor shall ensure the accuracy of the maintained assets and configuration items. Contractor shall conduct periodic audits and reviews of the assets and their configuration items to verify the accuracy and efficacy of the asset and configuration information. Contractor shall provide processes for corrective actions for exceptions, and ensure the completion of corrective actions.

The Contractor shall provide standards for the information required to be maintained on every CI type, and document those standards in the SMM. Contractor shall provide methods for identifying when standards are not met and supporting regular audits of CI records.

5.4.7.1 Asset and Configuration Management System

The Asset and Configuration Management System is a Service Management System. The Contractor shall manage and operate the Asset and Configuration Management System across all Integrated Service Providers providing Integrated Services. As part of that system, Contractor shall maintain the Asset and Configuration Management Database (CMDB) that will serve as the single source of information regarding assets and configurations for the Integrated Services, and other vendors. Contractor shall ensure that all asset and configuration information related to the Integrated Services resides in the SMS and CMDB.

The Contractor shall integrate with other SMS and CMDB of the Government, Service Providers, and other vendors as needed, and where directed by the Government. Contractor shall incorporate in the SMS and CMDB information from multiple databases that contains details of the components or CIs that are used in the provision, support and management of IT Services provided by the Integrated Service Providers and Government. Contractor shall consolidate data into the CMDB from other asset and configuration databases as necessary, and as directed by the Government. Contractor shall support the ability for bulk uploads and bulk updates, as approved by the Government.

The Contractor shall maintain proper authorization and control over CMDB data. Contractor shall maintain a secure audit trail of all CMDB transactions such that all changes are attributable.

The Contractor shall provide automated processes and use of discovery tools (e.g. inventory tools, validation tools, enterprise systems, network management tools) to load and update the

SMS and CMDB, while maintaining the auditability of transactions and approval of the Government.

The Contractor will provide for the maintenance of relationships between all service components and any related Incidents, problems, known errors, change and release documentation. Contractor shall map logical information to physical assets (e.g. applications, software, disaster recovery RTO/RPO, virtual server instance associations with physical hosts).

The Contractor shall facilitate and coordinate the updates of the SMS within designated timeframes with CI information for the defined services and assets under management and any other relevant information. Contractor shall provide efficient methods for Customers, the Integrated Service Providers, and other vendors to validate and correct data in the SMS and CMDB.

The Contractor shall provide Customers with online access to the SMS and CMDB. Contractor shall provide a customizable set of views for different stakeholders through the service life cycle for assets and configuration items.

5.4.7.2 Software Asset Management

The Contractor shall automate and facilitate workflow, tasks, process, tools and other general process items as a business practice to manage the entire software asset life cycle, from request through procurement, and operations management through metering and license control, and life cycle management, including upgrades, removal and disposal. The Contractor shall provide oversight and control of software configuration, distribution and license management processes and tools.

The Contractor shall manage compliance with all Software licenses in accordance with the SMM. Contractor shall track license counts and associations including all relevant details within the CMDB. Contractor shall confirm the presence and version of Software installed and that those attributes are recorded in the asset management system.

The Contractor shall coordinate and consolidate license compliance reporting across the Integrated Service Providers. Contractor shall provide for Service Provider specific processes that support the particular licensing associated with the Service Provider and the Customers' use of their contracted services.

The Contractor shall proactively manage the use of the Software in order to maintain strict compliance, including:

- Immediately notify and advise Customers of all Software license compliance issues associated with the Integrated Services and Customers retained Software
- For Customers retained Software, track and maintain the applicable licensing and use information received from Customers business units
- Provide reporting of license information and compliance to Customers, at least quarterly or as directed by Customers
- Report on Equipment with the presence of any unauthorized or non-standard Software
- Manage and track DOD and DHA PKI certificates

The Contractor shall track the life cycle of certificates in use in the environment including processes and procedures for renewals. Contractor shall provide notice to system owners of upcoming certificate renewals at least ninety (90) days in advance of expiration.

The Contractor shall maintain a secure Definitive Software Library (DSL) that logically identifies the master copy, physical and logical locations, and associated documentation for all Software associated within the EITS Environment, except those versions of Customers Application Software not released into the live environment. Contractor shall work with the Integrated Service Providers and the Government asset management to continually maintain the DSL.

The Contractor shall coordinate and facilitate the audit and verification of third parties for Software Asset Management, as identified by Government and Customers.

5.4.7.3 Audit and Verification

The Contractor shall perform and report on asset discovery, and other inventory verification audits, upon request from the Government. Contractor shall coordinate and manage inventory and asset verification activities across the Integrated Service Providers.

The Contractor shall perform initial and annual logical inventories of all hardware and software, including all virtual instances and network configurations. Contractor shall assist the Government in performing physical inventories, as requested by the Government.

The Contractor shall validate, on a quarterly basis, the currency of the CMDB against source information systems within other systems managed by the Integrated Service Providers. As part of the quarterly validation, Contractor shall perform logical and physical inspections.

The Contractor shall require and facilitate regular inventory reconciliation of the Service Providers' physical inventories, as defined in the SMM.

The Contractor shall conduct audits of CI records on a regular basis to ensure that records are complete with all required information, as defined in the SMM. Contractor shall provide analysis of audit results and verification, identifying exceptions in the CMDB data to the Government. Contractor shall open Problem tickets and initiate Continual Improvement items to address non-compliance.

5.4.7.4 Inventory Control

The Contractor shall establish an automated process to monitor, manage and control quantity, location and status of spare part and configuration item inventories, and facilitate workflow, tasks, processes, tools, and other general process items. This automated process will have significant interactions with DHA's Asset Management, Lifecycle Management, Incident Management, Change Management and Release Management processes, Configuration Management System, and Change Management Database (CMDB).

5.4.7.5 Technical Currency

The Contractor shall establish and manage the On-Going Program for Technical Currency that accomplishes the goals of Refresh and Software Currency and coordinates the activities of Government, Customers, Service Providers, and other vendors. This program produces and executes the Technical Currency Plan that ensures the execution of refresh projects and Software currency projects by the Integrated Service Providers.

The Contractor shall manage assets to be within the targeted currency as specified in the Technology Plan, which shall at a minimum specify the targeted age of all assets and the targeted release or version level of all software.

The Contractor shall develop a consolidated annual plan for Technical Currency (the Currency Plan) in coordination with the Integrated Service Providers, Customers, and the Government, and obtain approval of the Currency Plan from the Government and EITS Governance.

The Contractor shall work with Integrated Service Providers to coordinate, monitor, and manage the execution of Technical Currency responsibilities. Contractor and Service Providers will deploy Equipment and Software associated with any Refresh in accordance with the standards of the Technology Plan. Contractor and Integrated Service Providers will deploy equipment and software on the schedule of the Currency Plan, as approved by the Government and coordinated with the Customers.

5.4.8 Service Configuration Management

The Contractor shall implement a Service Configuration Management practice that contains information that relates to the maintenance, movement, and problems experienced within the operational environment. The Contractor shall provide a logical model of the EITS Environment by identifying, controlling, maintaining, and verifying information related to all Configuration Items (CI) and their relationships. Contractor shall actively work to model new relationships, identifying and creating CIs, critical attributes and relationships.

The Contractor shall implement processes that incorporate information from multiple sources containing details of components or CIs that are used in the provision, support, and management of its IT services. This information will also include maintenance, movement, and problems experienced with CIs.

The Contractor shall implement and maintain a Service Configuration Management process for all Integrated Services comprising the end-to-end services. Contractor shall conduct the Service Configuration Management process to identify, control, maintain, and verify the CIs approved by Customers, as comprising the Equipment, Software, and Applications to provide the Services. Contractor shall ensure:

- Accurate configuration data is maintained for the CIs used to provide the Integrated Services
- Only authorized CIs are accepted and recorded from receipt to disposal
- The configuration status of the CIs can be reproduced at any point in time throughout its life cycle

The Contractor shall implement controls to validate that any change to any CI records is the result of an approved Change.

5.4.9 Monitoring and Event Management

The Contractor shall provide and manage the Monitoring and Event Management practice for the integrated EITS Environment. Contractor shall implement and manage an integrated, proactive Event Management process so that all Integrated Services are monitored such that any Events occurring in the Integrated Services are identified, promptly actioned, recorded and reported. Contractor shall monitor the IT systems, infrastructure, environment, alarm

systems and environmental controls and take appropriate action to ensure no Event is lost or ignored. Contractor shall provide controls to ensure that monitoring is occurring in the EITS Environment as required (e.g. hardware monitoring from a Service Provider), and escalate areas where monitoring is not occurring to Government and EITS Governance.

The Contractor shall monitor for any change of state that has significance for the management of an IT service or other configuration item. The Contractor shall detect and take appropriate actions for escalation as defined in the SMM. The Contractor shall provide for end-to-end Event management across the Integrated Services with correlation between the Integrated Service Providers and other vendors as required to improve proactive response to Incidents and operational issues.

The Contractor shall manage and record all Events in an event log and maintain event log history in compliance with Government policies and rules.

The Contractor shall correlate Events to facilitate Problem Management and Root Cause Analysis of service failures. Contractor shall define and execute a process in which an alert, when needed, evolves into an Incident and is escalated for resolution. Contractor shall facilitate joint coordination meetings to address Events and to prevent unnecessary rerouting or reassignments of Events.

5.4.9.1 Event Management and Correlation System

The Event Management and Correlation System is a Service Management System. The Contractor shall manage and operate the Event Management and Correlation System across all Integrated Service Providers providing Integrated Services.

The Contractor shall maintain the Event Management database that will serve as the single source of information regarding known Events for the Integrated Services, and other vendors.

The Contractor shall facilitate and coordinate the update of the Event Management and Correlation System within designated timeframes with event information (e.g. event categories, event types, thresholds, defined actions) for the defined services and assets under management and any other relevant information, as directed by the Government.

The Contractor shall integrate with other event monitoring systems of the Government, Service Providers, and other vendors as needed. Contractor shall receive and handle Events generated from other sources (e.g. external network monitoring, third party surveillance).

5.4.10 Incident Management

The Contractor shall provide and manage the practice of Incident Management for the EITS Environment. Contractor shall provide an Incident Management process that will restore service operation as quickly as possible with minimum disruption to the mission, develop and document processes and procedures regarding interfaces, interaction, and responsibilities between various levels of support and any other internal or external persons or entities that may report an Incident, receive an Incident, or support the resolution of Incidents. Contractor shall monitor Incident details, status, and progress through to resolution.

The Contractor shall classify and prioritize Incidents as designated in Exhibit 3.4 (Severity Levels), or as designated in the SMM. Contractor shall ensure the Integrated Service

Providers execute the Incident Management process according to the agreed to prioritization model, and as described in the SMM.

The Contractor shall coordinate multi-domain tickets between the relevant Service Providers, other vendors, Customers, and Mission Partners.

The Contractor shall ensure the proper routing of each incident to the resolver, or resolvers, to ensure each incident receives immediate attention. Contractor shall coordinate Incident tracking efforts, and provide management and control of the Incident from identification to resolution. Contractor shall review the proposed resolution time with the appropriate stakeholders and update the status accordingly.

The Contractor shall oversee and coordinate restoration of normal service operations as quickly as possible, with minimum disruption to Customers' business operations. Contractor shall provide ongoing communications to Customers and key stake holders of changes in Incident status throughout the life cycle, and keep Customers informed of anticipated resolution times.

The Contractor shall coordinate conference calls with the necessary Integrated Service Providers and other vendors to appropriately triage the issue. Contractor shall facilitate and document Incident Management meetings (regular and ad hoc) to resolve high priority or languishing incidents.

The Contractor shall review the completeness of information for Critical Incidents (e.g. notes and work details) and perform a management review with Integrated Service Providers every week, and in accordance with the SMM.

Contractor shall develop, utilize, manage, and continually improve an inventory of defined and documented Incident models that enable swift response and resolution of Incidents. Contractor shall clearly document the tasks, actions, or steps to execute the Incident model and resolve Incidents. Contractor shall identify any required dependencies that must be considered in executing the Incident model. Contractor shall define other supporting information for executing the Incident model, such as: definition of responsibilities and roles, timescales, milestones and thresholds, and anticipated escalation points and escalation procedures.

The Contractor shall analyze Incident trends and make recommendations for reducing Incidents. Contractor shall advise Government on any new or changed information for the handling of Incidents. Contractor shall collate Incident information from authorized users regarding suggested improvements to the Integrated Services. Contractor shall provide all recommendations approved by the Government to Continual Improvement for implementation.

5.4.10.1 Major Incident Management

The Contractor shall provide a specialized process for Incidents that are deemed Major Incidents, which require swift recovery to serious interruptions of business activities and must be resolved with high degree of urgency. Contractor shall provide additional levels of communication and coordination for Major Incidents across the Integrated Service Providers, other vendors, Customers, and Mission Partners. Contractor shall identify Major Incidents by their impact or potential impact on the Customer, and by the urgency and priority of the Incident.

The Contractor shall create and manage the standard process for Major Incidents from identification through closure. Contractor shall identify and assign an Incident Manager that provides an appropriate level of dedicated attention to the Incident.

The Contractor shall formulate a cross-organizational team (scoped as appropriate to the type of Incident), in order to concentrate on this Incident alone to ensure that adequate resources and focus are provided to finding a swift resolution. The Integrated Service Providers and other vendors work under the EITSI Major Incident Manager, to support the leadership of the Government identified Battle Captain or Watch Officer. Contractor shall establish and provision any supporting conference bridges, on-line or on-site workspaces, which may be required to support the effective facilitation of Incident diagnosis and resolution.

5.4.10.2 Incident Management System and Knowledge Management Database

The Incident Management System and the central Knowledge Management Database are Service Management Systems. The Contractor shall manage and operate the Incident Management System and Knowledge Management Database across all Integrated Service Providers providing Integrated Services.

The Contractor shall implement and maintain the Incident Management System that will serve as the single source of information regarding Incidents for the Integrated Services. Contractor shall ensure that all information necessary to record Incidents, track Incidents, and support Incident Management is required and maintained, as identified in the SMM.

The Contractor shall provide for logging of all modifications to Incident Records, to provide full tracking, audit trail, and change control at the named-user level.

The Contractor shall integrate with other incident management systems of the Government, Service Providers, and other vendors as needed.

The Contractor shall implement and maintain the central Knowledge Management Database (KMD) that is used to capture, store, and retrieve information and solutions for reuse by the Integrated Service Providers, other vendors, and Customers.

At a minimum, Contractor shall collect information to populate the KMD based on the processing of Incidents, Service Requests, Projects, and On-Going Programs. Contractor shall ensure the KMD enables the sharing of policies, procedures, best practices, and the methods to resolve Incidents.

5.4.10.3 Incident Escalation

The Contractor shall provide a mechanism for expedited handling and increased communication of Incidents that are of high mission priority to Government, Customers, and other vendors, based on the assigned Severity Level, in compliance with the escalation processes described in the SMM.

Where Incidents are not resolved in the agreed time frame, Contractor shall provide a process for Customers and Service Providers to escalate to EITSI Management. Such process and supporting procedures will be defined and maintained in the SMM. Contractor shall ensure that the escalation process and procedures describe all relevant information on the Incident, such as: severity, impact, priority of the user, timeframes, and means attempted for resolution, and level of involvement of all parties.

The Contractor shall automatically prioritize high-impact Incidents, as defined by Government, such that they are treated with the highest priority.

The Contractor shall track information regarding escalations to include frequency of usage by Customers and Integrated Service Providers.

5.4.10.4 Incident Notifications

The Contractor shall provide regular progress notifications to Customers on current Incidents for all Severity Levels. The frequency of such notification will be determined by the severity of the Incident as determined using the definitions given in Exhibit 3.4 (Severity Levels), or as designated in the SMM. At a minimum, Contractor shall ensure notifications are made when an Incident or Service Request is created, suspended, and resolved.

The Contractor shall provide prompt notification to Customers of system outages on critical systems, as identified in the SMM, and provide affected authorized users with regular progress updates within designated timeframes, as prescribed in the SMM. At a minimum, Contractor shall ensure that such updates include: the nature and scope of the Incident, current estimated time to resolution, and potential short-term alternatives.

The Contractor shall provide for alternate methods of distributing notifications and communicating updates via various channels (i.e. not solely via e-mail).

5.4.10.5 Incident Management Reporting

The Contractor shall provide reporting on the effectiveness of Incident Management processes and trending of the practice; such reporting at a minimum shall include:

- Incidents Sources (by category, priority, service, and Service Level)
- Frequency regarding the types or categories of Incidents
- Durations of open Incidents (average and quantities by age)
- Incidents resolved upon first contact
- Trending of mean time to restore service (by category, priority, service, Service Level)
- Incidents not handed within Service Level targets (by category, priority, service, and Service Level)
- Incidents reopened (by category, priority, service, and Service Level)
- Incidents reoccurring (by category, priority, service, and Service Level)
- Incidents that have resulted in the creation of a Problem
- Incidents that were resolved by use of an Incident Model
- Association of Incidents by cause and resolution by Service Provider
- Number and percentage of Incidents escalated by organization, category, priority, and Service
- Customer escalation points

5.4.11 Problem Management

The Contractor shall provide and manage the practice of Problem Management for the EITS Environment. Contractor shall design and manage an integrated Problem Management process across the Integrated Service Providers to reduce the recurrence of Incidents. The Contractor shall manage the life cycle of all Problems using the Government furnished SMS

tools. The Contractor shall reduce the likelihood and impact of Incidents by identifying actual and potential causes of incidents and managing workarounds and known errors.

The Contractor shall analyze Incident records, and uses data collected by other ITSM processes to identify trends or significant problems. The Contractor shall minimize the adverse effect on the business of incidents and problems caused by errors in the IT infrastructure, applications, systems and supporting components, and will proactively prevent the occurrence of incidents and problems by identifying and eliminating causes of failure.

The Contractor will conduct regularly scheduled Problem Management meetings to prioritize the resolution of Problems with the Integrated Service Providers and Mission Partners and other vendors as identified by the Government. Contractor shall regularly survey Incidents to identify reoccurring Incidents for which the cause is unknown and any action that can be taken to identify the root cause and resolution.

The Contractor shall implement controls to validate that Problem resolution and corrective actions taken are sufficient to address the Root Cause fully and that it does not reoccur. This includes the update of manuals, procedures, and other documentation. Contractor shall define the criteria for prioritization of Problems, in accordance with the Severity Levels. Contractor shall validate and submit Problem resolution and remediation methods for inclusion in the Knowledge Management database, as documented in the SMM.

The Contractor shall implement measures to avoid unnecessary reoccurrence of Problems. This includes initiating Change Management to remediate faults in the IT Infrastructure, processes, services, and application systems. Contractor shall escalate to appropriate management within the Service Providers and Customers if corrective actions are not being taken.

The Contractor shall coordinate Problem tracking efforts and notifications to the Service Desk and Service Providers, and maintain regular communications between all parties until Problem is resolved. Contractor shall provide communications to Customers and, as necessary, affected authorized users and to Service Providers, from the time a Problem is identified through to resolution. As necessary, also providing any follow-up communications and reporting required post-resolution.

The Contractor shall provide a process for Government, Customers and Service Provider(s) to escalate Problems. Contractor shall ensure such escalations are according to processes and procedures documented in the SMM.

5.4.11.1 Root Cause Analysis

The Contractor shall provide Executive Summaries and other Root Cause Analysis (RCA) to support Customer understanding of events in the EITS Environment. Contractor shall implement a standard process across all the Integrated Services and provide RCA reporting as documented in the SMM.

The Contractor shall be responsible for the delivery of RCAs, and shall facilitate and orchestrate the RCA process from initiation to closure with the Integrated Service Providers:

- The EITSI will initiate an RCA for all Severity 1 Incidents
- The EITSI will initiate an RCA when requested by Government or Customers

The Contractor shall provide standard tools, forms, and criteria for documenting RCAs, as approved by Government. Contractor shall ensure that all appropriate roles are engaged to perform the RCA process, including, but not limited to Government, Customers and Service Providers.

The Contractor shall track all RCA activities and provide for an RCA Coordinator to act as the day-to-day interface into the RCA process. Contractor shall coordinate, require, and facilitate the closure of RCAs that require increased focus to meet committed service levels. Contractor shall provide a process for Government and Customers to escalate non-performing RCAs, as required.

5.4.11.2 Problem Management System and Known Error Database

The Problem Management System and Known Error Database are Service Management Systems. Contractor shall manage and operate a Problem Management System, and a Known Error Database across the Integrated Services that will serve as the single source of information regarding Problems. Contractor shall provide Customers and Service Providers with the ability to enter Problem records directly into the Problem Management System and known error records directly into the Known Error Database. Contractor shall develop tools, scripts, and enhanced processes to proactively perform Problem Management, with the objectives of automating the Problem Management process and predicting Problems before they occur.

5.4.12 Service Request Management

The Contractor shall implement and manage the Service Request Management practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall assist in the coordination of requests for Integrated Services and other program related services from authorized users. Contractor shall ensure service requests are managed from the initial request through fulfillment or cancellation from multiple sources, such as Service Providers, other vendors, and Customers. While the majority of Service Requests are minor (such as standard changes), the Service Request Management practice shall direct more complicated requests to the solution design process.

5.4.12.1 Service Request

The Contractor shall provide a standard process for service requests to support the receipt, submission, acceptance, approval, and fulfillment or cancellation of these requests. This includes coordination for gathering requirements, validation of technical means, and budgetary information, with relevant domain groups (e.g. architecture, engineering, service management) within the Integrated Service Providers and Customers.

The Contractor shall execute Service Request Management to achieve its primary purpose to fulfill service requests within the agreed Service Levels and timeframes, and to promote Customer and user satisfaction. Contractor shall establish processes that properly routes and prioritizes Service Requests across multiple organizations (e.g. Integrated Service Providers, other vendors, Customers) and ensures appropriate approvals as outlined in the SMM.

The Contractor shall develop and document processes and procedures regarding interfaces, interaction, and responsibilities between support personnel (e.g. tiers or levels of support),

and any other internal or external persons or entities that may support the fulfillment of Service Requests.

The Contractor shall integrate with fulfillment systems of the Government, Service Providers, and other vendors as needed.

The Contractor shall establish processes and criteria to support expedited handling of Requests. Contractor shall expedite the handling of Requests from specific designated users or as authorized by Government.

The Contractor shall track the progress of fulfillment efforts and the status of all Requests, and ensure information on Requests is updated within designated timeframes to support a current and accurate view of Service Requests.

The Contractor shall provide and maintain regular communications as required until Request is fulfilled or cancelled and document the communications as required. The frequency and nature of such communications will be in compliance with Service Request policies and procedures as documented in the SMM.

The Contractor shall provide anticipated completion times for active Requests and update notification systems as required in the Service Request Management processes to keep Customers informed. Contractor shall keep Government and Customers informed of any issues with the completion of Requests and status changes throughout the Service Request life cycle. When a Request cannot be completed in the committed timeframe, Contractor shall provide a revised completion time after consultation with the requesting Customer.

The Contractor shall review Service Request prior to closure or cancellation to ensure proper categorization, documentation, confirmation of completion and activities required to initiate other appropriate actions (e.g. asset and configuration updates, disaster recovery updates).

5.4.12.2 Solution Request

The Contractor shall provide an effective Request for Solution (RFS) processes and appropriate mechanisms for fulfilling complex service requests, requirements gathering coordination with the customer, design, pricing, solution, and proposals; including appropriate communications to adequately set expectations and promote good customer service. Contractor shall work with the Integrated Service Providers and other vendors as required to formulate a complete solution and proposal. Contractor shall ensure all RFS are solutioned in compliance with Government policies and rules as outlined in the SMM.

The Contractor shall effectively leverage existing infrastructure and designs for the most efficient and effective cost solutions, provide technical guidance to Customer, and architect solutions through coordination with the Integrated Service Providers and Customers.

The Contractor shall develop standard proposal mechanisms and processes for formulating solution proposals and obtain appropriate Government and Customer approvals, as detailed in the SMM. Contractor shall provide all necessary materials and artifacts to Government or the Customer for understanding of the proposal. Contractor will provide a timeframe to the Customer for delivering a solution once requirements are accepted by Customer. Contractor will provide proposal responses and reworked proposal responses in a timeframe required by the Government.

The Contractor shall develop a Request for Estimate (RFE) processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution but includes a Rough Order of Magnitude (ROM) estimate of schedule and costs. All ROM estimates will align to Course of Action (COA) and a technical overview or architecture of the COA.

Requirements gathering coordination and preparation of RFS and ROM proposals are at no additional charge to Government.

5.4.13 Service Design

The Contractor shall implement and manage the Service Design practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall analyze requirements and service requests from the Government and recommend new services as well as changes and improvements to existing services.

The Contractor shall implement and manage the Service Design process as documented in the SMM. This process is designed to ensure that a successful and repeatable methodology is applied to the design and transition phases before introduction into the EITS Environment. Contractor shall manage Service Design process across the Integrated Service Providers to be timely, efficient, and cost effective.

5.4.13.1 Design Coordination

The Contractor shall coordinate all service design activities, processes, and resources. Contractor shall ensure the consistent and effective design of new or changed IT services, service management systems, architectures, technology, processes, information, and metrics.

5.4.13.2 Service Transition

The Contractor shall coordinate the development and deployment of IT services ensuring changes to services and Service Management processes are coordinated and implemented as existing IT services are retired, modernized, or new IT services implemented.

5.4.14 Service Validation and Testing

The Contractor shall implement and manage the Service Validation and Testing practice across the Integrated Service Providers and other vendors, as directed by the Government. The Contractor shall perform testing to ensure that engineered solutions meet technical requirements and Customer expectations. Contractor shall verify that IT operations are able to support the Service as implemented (e.g. new services, additional services, projects, releases, and major changes).

The Contractor shall design and establish an integrated Service Validation and Testing (SV&T) process to ensure changes to the Integrated Services are tested and fit for purpose and use. The design of the testing controls and any changes to that design are subject to Government approval. Contractor shall integrate the SV&T process with its other service management processes, especially Release Management, Deployment Management, Change Enablement, Asset and Configuration Management, and IT Service Continuity Management.

The Contractor shall create SV&T plans, controls, pilot sites, and checklists to validate service readiness. Contractor shall obtain Government, or designated Customer approval on

the required level of validation and testing. Contractor shall integrate each Integrated Service Provider's testing process for changes in services with Customer SV&T process, where the processes interact.

5.5 Technical Management Practices

The Contractor shall implement and maintain the following technical management practices, as described for ITIL 4 under Technical Management Practices, and as approved by the Government.

5.5.1 Deployment Management

The Contractor shall ensure the accuracy and compliance with processes for moving any Software, hardware, Equipment, documentation, and any other service components to live environments to include non-destructive "roll back" processes in the event of a deployment failure.

5.5.1.1 Pre-Deployment Testing

The Contractor shall plan for an integrated pre-production test, and ensure the completion of such pre-production testing, prior to migrating a system or service into production for the EITS Environment. Contractor shall incorporate into their pre-production testing the pre-deployment systems test plan developed by the Service Provider assigned majority responsibility for the release or deployment. Where such a pre-deployment systems test plan does not exist, or where a Service Provider does such not have majority responsibility, the Contractor shall create the pre-deployment systems test plan.

The Contractor shall provide for pilot activities as part of their pre-production test, where appropriate or as requested by the Government.

The Contractor shall provide a process for managing pre-deployment testing and document the process in the SMM. Contractor shall ensure compliance with the pre-deployment testing process across the Integrated Service Providers. As part of this process, Contractor shall accomplish independent quality assurance that verifies the change, release, and deployment plans in order to identify risks, issues, and deviations related to any significant new or changed service. Contractor shall facilitate and coordinate the Integrated Service Providers in prioritizing risks, issues, and identifying deviations.

The Contractor shall perform quality assurance of the service management processes and tools to ensure operational readiness such that the new or changed service can be operated and maintained effectively (i.e. fit for purpose and use). Contractor will verify:

- The ability of the Service Providers to respond to and resolve Incidents
- The accuracy of Configuration Item data
- That systems are under monitoring and reporting tools
- That operating procedures, training, and documentation is accurate
- That service continuity provisions are ready
- That security management and patching levels are accurate

The Contractor shall coordinate the resolution of test failure issues, including platform-integration-related issues with the appropriate Integrated Service Provider.

The Contractor shall create and submit a Pre-Production Validation report to Change Management, showing the result of the pre-production test conducted by the Integrated Service Providers and the results of Contractor's independent quality assurance measures. Contractor shall consolidate and provide test reports to Government and Customer that outlines test outcomes and actions being taken to address failures. Contractor shall validate that the quality assurance measures were completed to Customer's satisfaction. Contractor shall obtain any required approvals to release to production.

5.5.1.2 Post-Deployment Support

The Contractor shall establish a post-deployment support function to accept end-user complaints, answer questions, and provide for identifying remaining defects in the deployment and actioning those defects with the Integrated Service Providers for resolution. Contractor shall monitor and review the activities for resolving outstanding defects to Customer's satisfaction.

The Contractor shall provide for expedited Change Enablement practices that support the swift resolution of defects for the Post-Deployment activities.

The Contractor shall document and make available for re-use the frequently asked questions from deployment.

5.5.2 Engineering Management

The Contractor shall recommend operational guidelines that establish process-based methodology for investment assessment of DHA's new and/or evolving technical service offerings. The Contractor shall:

- Receive, review, and assess mission and project requests
- Provide recommendations for acceptance into service design process
- Align engineering services and solution design in support of all infrastructure change efforts that may involve delivery of new capability or fulfillment of corrective or preventative measures
- Alignment of engineering services with other processes including change, incident, problem, and availability management as well as continual improvement
- Work in close coordination with Architecture Management and other Technical Subject Matter Experts (SMEs) to evaluate new technology that meets emerging IT or service strategy or adds resiliency in existing IT service delivery infrastructure

5.5.3 Technical Subject Matter Experts

The Contractor shall provide Technical Subject Matter Experts (SME) in multiple Information Technology (IT) domains and be responsible for coordinating and facilitating communication of IT tasks, between IT engineers and system operators.

5.6 Customer Interfaces

The Contractor shall coordinate all interactions with MHS Customers and Mission Partners.

Interactions should optimize customer and Mission Partners interfaces, to better understand and react to customer needs and experiences. Customer interfaces are any interaction (e.g. tool, call or personal interaction) that Customers experience with the Integrated Services.

5.6.1 Business Relationship Management

The Contractor shall provide identification and response to Customer IT needs to ensure appropriate services and capacity are developed to meet customer needs and expectations through a proactive and positive practice of Business Relationship Management. The Contractor shall identify the IT needs of MHS customers and ensures that appropriate services and capacity are developed to meet those needs.

The Contractor shall posture a positive relationship with DHA customers and Mission Partners to foster and align a strong business relationship maximizing customer satisfaction and value perception. A strong business relationship shall be established with the end-user customer by understanding the customer's mission and their desired outcomes. As part of this practice, Contractor shall facilitate consistent alignment of specific Contractor Personnel to specific Customers. The Contractor shall coordinate with DAD IO/J-6 to navigate all elements of service introduction on behalf of customers.

The Contractor shall provide a single point of contact as liaison for Customers on the function of the Integrated Services and the quality of the delivery from the Integrated Service Providers and other vendors. Contractor shall provide personnel that demonstrate knowledge of the Customer, the Customer operating environment, and Customer mission drivers.

As part of that role, those Contractor Personnel shall:

- Coordinate a regular review of the Service Portfolio with the Customers and other entities as required by EITS Governance
- Collect Customer mission concerns, upcoming activities and changing priorities, and provide meaningful insight into the Customer mission needs and activities back to EITS Governance
- Support the communication activities of Government and Customers, as required
- Provide a point of escalation on service delivery issues
- Demonstrate the ability to drive change and resolve challenges in the delivery of services, within both the Contractor and Service Providers organizations
- Regularly update documentation on the mission objectives and organization of Customers and make documentation and training available for the use of Contractor, Service Providers and Government

The Contractor shall convene and conduct regular Customer operations meetings that include the Contractor single point of contact and Customer representative(s) in order to understand, monitor and collaborate on service provision to continually improve the customer experience. Meeting cadence to be determined by each Customer. Depending on the specific agenda, Contractor may invite representatives of one or more Service Providers to attend.

5.6.1.1 Customer Experience Management

In collaboration with the Government, the Contractor shall establish a robust Customer Experience Management Program focused on optimizing the Customer Experience over time. Contractor shall employ a variety of tools, metrics, and tactics to measure, analyze and

continually improve both the Customer Experience and the maturity of delivery for the Integrated Service Providers and other vendors. Customer Experience Management is an On-Going Program.

The Contractor shall collect, consolidate, analyze, and summarize Customer Satisfaction Survey results to be presented as a consolidated view to EITS Governance.

The Contractor shall work with other Service Providers and the Government in the development of the Customer Satisfaction Surveys and defining the survey implementation strategy.

5.6.1.2 Customer Satisfaction Surveys

The Contractor shall provide for Customer Satisfaction Surveys for multiple stakeholder groups, including:

- DHA Executives
- Customer IT Leadership
- Mission Partner IT Leadership
- DAD IO/J-6 IT Leadership/Staff
- Point-of-Service Customer Satisfaction Survey

The Contractor shall develop draft surveys in cooperation with the Government. Contractor shall distribute Government approved surveys to stakeholder groups and statistically valid samplings of such groups. Contractor shall conduct such surveys on a frequency defined by the Government. Contractor shall encourage participation using tools and techniques agreed to by the Government to ensure statistical validity of all surveys.

The Contractor shall allow adequate time for response that encourages participation and full responses. Contractor shall retain survey results to allow for trend analysis over time. Contractor shall provide the Government with complete survey data for its verification of results. Contractor shall compile and analyze survey results and make recommendations for improvements.

The Contractor shall develop and execute plans to implement improvements, as approved by the Government. Contractor shall provide Government approved recommendations to the Continual Improvement practice.

5.6.1.3 Customer Experience Measures

In order to fully understand and optimize the customer experience, Contractor shall establish a performance management framework that includes perception, descriptive and outcome metrics including specific reports, service levels and Customer Satisfaction measures. These metrics will then inform the choices made for follow-up activities (e.g., focus groups, improvement projects). Contractor shall work with the Government to propose the framework approach and shall implement the Government approved framework.

The Contractor shall consolidate measures into a single display available through the Customer Portal. Contractor shall perform analysis of the consolidated measures and provide recommendations to the Government. Contractor shall participate in work sessions with stakeholders (e.g., EITS Governance, Customers, focus groups) to discuss overall results and

develop specific action plan. Contractor shall facilitate and provide logistical and administrative support to these work sessions, where requested by the Government.

5.6.2 Business Analysis

The Contractor shall formulate recommendations on technical innovation across the Integrated Services to improve mission aligned IT service quality. Technical innovation will be based upon the captured results from process evaluation, service measurement, and quality assurance programs and the Improvement Planning activities.

The Contractor shall incorporate approved recommendations and maintain them in the SMM, Service Catalog, Service Definition Documents, and other documents as appropriate.

5.6.2.1 Innovation Plan

The Contractor shall identify areas of innovation to improve service delivery alignment to Customer mission needs across the Integrated Services through a consolidated Innovation Plan, and shall facilitate and coordinate the Integrated Service Providers in execution and implementation of the plan. Contractor shall deliver an updated the Innovation Plan annually.

The Contractor shall align activities identified in the Innovation Plan, to the Technology Plan, the Cyber Security Plan, the Technical Currency Plan, Customer mission strategies and needs, forecasts from Service Portfolio Management, Demand Management, and other analyses and priorities as directed by Government.

The Contractor shall ensure the Innovation Plan includes, at a minimum: the desired outcomes from Customers as they are identified and refined, the implementation status of each proposal delivered under the previous plans, and a narrative and schedule for the activities the Contractor and Service Providers will undertake in order to deliver on the desired outcomes of the Innovation Plan.

At least twice a year, the Contractor shall coordinate and facilitate a forum for innovation of the Integrated Services with Customers. Such forum will include participants as directed by Government and EITS Governance.

5.6.3 Demand Management

The Contractor shall coordinate with Customers to determine their demand for services and seek mechanisms to meet these demands. The Contractor shall conduct an analysis of patterns of activity and service usage and involve resource rationalization mechanisms to encourage shifts in demand.

The Contractor shall encourage Customers to make the most effective use of the Integrated Services and Contractor resources and to assist in minimizing costs to the Government while maximizing the value Customers receive from the Integrated Services. Such assistance shall include coordinating, collating, and reporting evidence of Demand reductions from the Service Providers.

The Contractor shall align the supply of the Integrated Services to the demand for those services by coordinating, collating, and reporting predicted and actual consumption of the Integrated Services as provided by the Service Providers on a monthly basis.

The Contractor shall track patterns of business activity across the Integrated Services on and identify trends and risks that may cause demand to exceed the available capacity of the Integrated Service Providers.

The Contractor shall integrate Demand Management with other ITIL 4 practices (e.g., Capacity Management, Service Level Management) in order to manage long-term demand for the Integrated Services and to identify and resolve over or under-utilization issues.

The Contractor shall establish processes for gathering and forecasting Customers' project requirements in coordination with Government, Service Providers, and other vendors.

5.6.4 Customer Portal and Reporting

The Customer Portal is a Service Management System. The Contractor shall develop, implement, and manage the Customer Portal as the centralized point of access to all SMS, documentation, SMM, and information pertaining to the delivery of the Integrated Services, for Customers, Service Providers, and the Government. This will include access to Service Reporting and a customizable dashboard of services appropriate to the Customer. Contractor shall enable differentiated access for the various entities utilizing the Customer Portal (e.g. DHA, Customers, Mission Partners, and Integrated Service Providers), including role-based assignment of views and functions.

The Customer Portal will provide authorized users with access to the SMS, to execute common user functions, such as: create an Incident or Service Request, check on the status of their Incident or Service Request, add a note to any open Incident or Service Request in their name, view and submit feedback on Self-Help articles, or view a list of critical incidents currently impacting their organization.

Contractor shall provide training for the Customer Portal and dashboard to Customers, Integrated Service Providers, Government, and other designated authorized users.

Contractor shall update information in the Customer Portal in a timely manner. The frequency of updates for elements and subcomponents of the Customer Portal will be documented in the SMM.

5.6.5 DHA Global Service Center

The Contractor shall provide a strategic central point of contact for Customers regarding the Integrated Services. The Contractor shall manage and support information delivery across all the ITIL 4 practices for Service Operations (e.g. Event Management, Incident Management, Problem Management, Request Management, Access Management) and is a central focus for the DAD IO/J-6 strategy.

The Global Service Center supports the ITIL 4 practices for Service Management by providing an operational single point of contact to manage information, communication, and service delivery. The Contractor shall operate a tiered support structure as approved by the Government. The tiered structure shall consider multiple tiers such as customer self-service, empowering service desk resolution capability, quick hand-off to other delivery partners, and shift-left capabilities.

5.6.5.1 Service Desk Services

The Contractor shall facilitate contacts for authorized users for both inbound and outbound support (e.g. contacts to other levels of support, vendors, and support groups). Authorized users can call the Service Desk for all Integrated Services.

The Contractor shall manage all contacts from authorized users relating to the Integrated Services, including, but not limited to, the following:

- Log all relevant details, within an Incident or Service Request, in the appropriate Service Management System (SMS)
- Assign categorization, severity, and prioritization, as documented in the SMM.
- Provide first-line investigation and triage in an attempt to resolve Customer issues
- Provide routing of Incidents to appropriate resolver groups in a timely fashion
- Escalate Incidents and Service Requests that are not resolved within the agreed upon Service Level
- Communicate with authorized users by keeping them informed of Incident and Service Request creation, suspension, tasks requiring their action, resolution, and closure
- Ensure resolution of all tickets (e.g. Resolved Incidents, Completed or Cancelled Service Requests) from contacts in accordance with the SMM
- At resolution, ensure all relevant details are documented within the SMS ticket (e.g. the resolution, resolution method, user acceptance)
- Retain overall responsibility and ownership of all Incidents and Service Requests from the time the ticket is created until they are closed or cancelled
- Ensure that the Service Desk is available at all times (i.e. 24x7x365).
- Support the use of multiple methods of contact for authorized users, including at a minimum phone calls, email, chat, and web entry, as well as other methods as approved by the Government
- Ensure that each work shift has a turnover process to update the next work shift regarding status of key incidents, incident hand-offs and general knowledge transfer to ensure that Customer problems are resolved in a timely manner
- Promote efficient use of Service Desk resources through Continual Improvement (e.g. enhancements of Customer Portal, increased self-help functionality)
- Provide processes and controls to enable entitlement and identification of authorized users, as approved by Government
- Provide processes to support the use of Customer provided Service Desk attendant scripts that include Customer specific scripts as required, for supporting Incidents and Service Requests related to the Integrated Services (e.g. Customers specific Applications, systems, sites)
- Provide a means for authorized users to provide feedback, via a survey, upon ticket resolution
- Develop and document processes regarding interfaces, interaction, and responsibilities between differing support levels, and any other internal or external persons or entities (e.g., Customer application support) that may either submit or receive a ticket
- Provide for correlation of Events and Incidents for proactive actions. Contractor shall investigate related Events from the Event Correlation and Monitoring System.

Contractor shall investigate related Incidents from the Incident Management System. Contractor shall provide analysis to create any required Incidents and Problems

- Provide an effective means of using industry recognized methods to determine, measure and monitor Service Desk staffing levels, requirements, and allocations. Contractor shall provide processes for the continuous evaluation (e.g. ticket and call quality) of Service Desk personnel on behalf of the Government and Customers
- Ensure the Service Desk communicates to authorized users in English, using terms that are clearly understood by the authorized users and consistent with those used by Government.
- Conduct continual improvement activities to review the effectiveness of Service Desk processes and procedures. Contractor shall conduct regular independent quality assurance reviews of call resolutions and other actions taken by analyzing SMS ticket data to identify correlations between events and incidents, and to predict potential problems
- Provide resources in response to surges or spikes in incident volume that may occur throughout the performance of Contractor Services

5.6.5.2 Tiered Support

The Contractor shall provide and manage a tiered support for the management and distribution of tickets that support the EITS Environment.

The Contractor shall provide analysis of the current use of tiered support in the EITS Environment and provide advice on an effective tiered support structure that takes into account: multi-provider environment, the multiple businesses of MHS, the multitude of other vendors in the environment, and the businesses of Mission Partners. Contractor shall implement the tiered support structure, as approved by the Government. As part of the recommendation, Contractor shall demonstrate how the tiered structure supports:

- Self-service efficiencies
- Heightened customer satisfaction
- Call handling and first-call resolution
- Shift-left capabilities to empower service desk
- Seamless ticket handling to different support entities
- Deep expertise available as appropriate
- Escalate tickets between service tiers
- End-to-end ownership of tickets by the Global Service Center

5.6.5.3 Knowledge Database

The Knowledge Database is a Service Management System. The Contractor shall manage and operate the Knowledge Database in support of the Global Service Center and all Integrated Service Providers providing Integrated Services.

The Contractor shall ensure that the Knowledge Database is accurate, compliant, and accessible by all authorized users and Integrated Service Providers. Contractor shall provide input and feedback to the Knowledge Database based on analysis of contacts, Incidents and Problems.

The Contractor shall curate the content of the Knowledge Database to ensure that articles are current. Contractor shall review the contents on a regular basis, refine articles when appropriate, and appropriately retire articles when no longer relevant.

The Contractor shall conduct Continual Improvement activities to review Knowledge Database articles.

5.6.5.4 Service Desk Frequently Asked Questions

The Contractor shall provide and routinely update, in accordance with the SMM, a list of Frequently Asked Questions (FAQ) regarding the Integrated Services on the Customer Portal. Contractor shall provide information as part of FAQ to enable authorized users to increase self-help and their ability to resolve Incidents and reduce Service Requests. Contractor shall ensure that published FAQ information is subject to approval by Government.

The Contractor shall provide recommendations for better use of FAQ and other Customer self-help tools to improve Customer service. Contractor shall provide approved recommendations into the Continual Improvement practice.

5.6.5.5 Service Desk Telephony System

The Service Desk Telephony System is a Service Management System, provided by the Government to Contractor. Contractor shall manage and operate the Service Desk Telephony System to manage all calls and other contacts to the DHA Global Service Center.

The Contractor shall manage and maintain the system documentation for the SMS and ensure its accuracy to support system maintenance, as directed by the Government. Contractor shall be responsible for the RMF and maintain the ATO for the Service Desk Telephony System.

The Contractor shall provide that all Calls may be recorded, and made available to the Government, for an agreed upon period of time.

As part of the Service Desk Telephony System, Contractor shall manage and configure:

- Automated call routing and call flows
- Call handling logic and ongoing tuning
- Queue management
- Skill management
- IVR logic and verbiage modification
- Voice recognition database
- Skill creation and modification
- Computer telephony integration
- Custom configuration supporting unique Customer applications and processes
- Telephony System reporting

The Contractor shall provide for logging of all modifications to the Service Desk Telephony System, to provide full tracking, audit trail and change control at the named-user level.

The Contractor shall produce trend reports for the Government to highlight underlying SMS issues, emerging risks and responding proactively to potential areas of weakness or concern.

The Contractor shall provide advice and direction to the Government for planning for the use of the SMS (e.g. site expansion, data center usage, office space).

The Contractor shall provide remote or alternate site integration and application extension for virtual contact center deployment and Continuity of Operations capabilities.

5.6.5.6 Service Desk Reporting

The Contractor shall provide daily, monthly, and as requested ad hoc reports to Government on Global Service Center activities and performance, which at a minimum includes:

- Key issues relating to Service Desk processes, improvements, script development.
- Status as to Service Desk staffing, training, and authorization.
- Integration activities and issues with other Service Desks belonging to Customers and Service Providers as directed by Government.
- Trend analysis during the thirteen (13) most recent months, including:
    - Number of contacts, to include all methods of contacts (e.g., calls, email, web, chat)
    - Percent of calls abandoned, % of tickets resolved, average speed to answer, average call duration, and average time to abandon
    - Number and percentage of contacts passed to other Service Desks.
    - Daily and month-to-date numbers for Incidents and Service Requests by priority.
    - Aging reports of tickets left unresolved

The Contractor shall provide other reports as needed regarding Global Service Center operations and performance, as directed by the Government, and the reports described in Exhibit 3.3 (Reports Matrix).

5.6.6 Service Catalog Management

The Contractor shall organize and curate a collection of business and information technology related services that are reflective of the existing and ever-changing service baseline. Contractor shall provide descriptive, entitlement, costing, and other criteria for consumption-based provisioning and may be constructed to provide contextual-based content displayed in any number of self-provisioning portals, including storefront or purpose-built request management portals for strategic initiatives. The Contractor shall deliver Service Catalog Management services for all Integrated Services, and select other services provided by Government, other vendors, and Customers.

The Contractor shall proactively support Government and Customers with resource, expertise, and advice in aligning the Service Catalog with Customer strategic direction, technical architecture, refresh strategy, and product evaluation. Contractor shall ensure that all services published in the Service Catalog have been approved in accordance with EITS Governance. Contractor shall coordinate with Government to ensure service priority and service level requirements are met.

The Contractor shall ensure all changes to Service Catalog are approved by Government and EITS Governance.

The Contractor shall implement all Government approved updates to the Service Catalog within the timeframes approved by Government and as specified in the SMM.

The Contractor shall distribute updates to Customers on all changes for the Service Catalog including planned changes and implemented changes.

The Contractor shall proactively provide technical and commercial recommendations to Government and Customers on both content and structure of the Service Catalog.

The Contractor shall establish and maintain effective links and integration between the Service Catalog and the Asset Management and Configuration Management systems (e.g. CMDB).

The Contractor shall ensure that all authorized users have appropriate access to the Service Catalog, as defined by Customer. Contractor shall perform access reviews in accordance with the SMM.

The Contractor shall develop the Service Catalog to ensure that the content of the Service Catalog is easily accessible and available in a user friendly format. Contractor shall ensure that visibility of the Service Catalog is relevant to the Customer and the user's role, as defined by the Customer.

The Contractor shall require and facilitate the means of automating the ordering of items in Service Catalog with the Integrated Service Providers.

The Contractor shall track and manage the life cycle of products and services in the EITS Environment. Contractor shall document those products and services that are non-orderable due to service life cycle stage (e.g. services in pre-production or in retirement stages).

5.6.6.1 Service Catalog System

The Service Catalog System is a Service Management System, provided by the Government to Contractor. Contractor shall implement, make available to Customers, and operate this Service Catalog System for the compilation, collation, maintenance, and publishing of the requests for Integrated Services and other services identified by Government.

The Contractor shall configure and maintain the Service Catalog System to support request orders and fulfillment from Customers including automated workflow for approvals as defined in the SMM. Contractor shall work with Customers to authorize their designated users and other users for approval. Contractor shall implement and maintain workflows for each Customer business unit that enables an effective and timely approval process, by those users who are authorized to make such approvals.

The Contractor shall support capturing appropriate input attributes for the fulfillment of orders from authorized users (e.g. Configuration Item information, site, user name) as required by the fulfilling Integrated Service Provider.

The Contractor shall implement and maintain self-service capability for Customers to find status information on orders, including information on the fulfilling Integrated Service Provider orders or supporting sub-orders.

5.6.6.2 Service Catalog Contents

The Contractor shall ensure that the Service Catalog includes all services and sub-services available to Customers. Contractor shall coordinate with the Integrated Service Providers to collate and publish all such service items as the Service Catalog.

The Contractor shall establish processes and SOPs in the SMM for updating the Service Catalog contents. Service Catalog content shall be reviewed and updated in accordance with the SMM, and at no less than a monthly basis.

The Contractor shall ensure that all product and service descriptions in the Service Catalog have sufficient detail on mission value, features, technical specifications, costs, inventory availability, delivery time and options to enable an authorized user to make an informed choice. Contractor shall ensure that service descriptions and all associated metadata is accurate and up to date.

The Contractor shall ensure any additional costs or recurring costs are included in the detail description (e.g. a requirement to purchase supporting products or services to install, support or maintain the item ordered from the Service Catalog).

The Contractor shall categorize the content of the Service Catalog to enhance usability of the catalog (e.g. configuration, Equipment, software, service) as appropriate. Contractor shall work with Service Providers to define the schema for categorization in the SMM, as approved by the Government.

The Contractor shall provide detail of all required or optional supporting processes for any Service Catalog Item.

The Contractor shall provide capability to include all Standard Catalog Items from any Integrated Service Provider.

The Contractor shall ensure the Service Catalog contents will include any notation required for specific use (or limitation) of each Service Catalog item by region, Customer, business unit, project or category of user.

The Contractor shall proactively inform Customers if any Catalog Item requires Customer's approval authority other than financial (e.g. health, safety or security restrictions).

The Contractor shall ensure that spare or surplus assets are included in the Service Catalog and available for ordering.

The Contractor shall provide for management of life cycle information to support the other areas of Service Delivery within the Service Catalog (e.g. Service Design, Refresh, and Technology Planning) for order by authorized users, as authorized by Government.

5.7 Global Operations

The task items under Global Operations require Contractor to provide services much like the Service Providers and other vendors in the EITS Environment. As such, the requirements may refer to the Contractor working with the EITSI. In this case, the Contractor will be performing two roles, that of the EITSI and that of a Service Provider. Contractor shall document in the SMM the processes and interactions between its core EITSI functions and the tasks conducted under Global Operations. The Contractor shall ensure the activities it conducts under Global Operations are held to the same standards of operation as other Service Providers.

The Government may transition one or more of the items under this Task from the Contractor to a Service Providers or other vendor. When so directed, Contractor shall cooperate and facilitate the transition of those responsibilities under this Task to the Government designated

Service Provider or other vendor. The Contractor shall support Global Network Operations and the SIPRNet Operations to provide 24x7x365 mission critical IT operational services. Contractor shall appropriately and seamlessly integrate the Global Network Operations and SIPRNet Operations into their delivery of cross functional services and other Contractor Services as identified in this PWS and any Call Orders.

The Contractor shall document and maintain service performance characteristics for Global Network Operations and SIPRNet Operations within the SMM. Contractor shall document operating environments and diagram operating environments to the policies documented within the SMM and as directed by Government.

The Contractor shall provide support for data source integration from multiple systems including the ITSM System, Service Desk Telephony System, and enterprise monitoring tools. Contractor shall develop and deploy additional interfaces as required and where directed by the Government.

5.7.1 Circuit Management

The Contractor shall provision MHS circuit as requested by authorized users through the EITSI managed Service Request practice. Contractor shall coordinate with Customers for the full life cycle of circuits; including: provisioning, discontinuing, changing, tracking, billing, and overall management of circuit infrastructure. Contractor shall verify circuit technical parameters with Customers. Contractor shall provide circuit cost estimates to Customers as requested.

The Contractor shall verify funding availability for circuit requests through the designated Government representative and processes and track funding through to completion of the request.

The Contractor shall document and maintain DHA policies, processes, procedures, and SOPs for circuit management in the EITSI provided SMM, as directed by the Government. Contractor shall adhere to the SMM and the ETSI managed practices for the Integrated Environment.

The Contractor shall interface with Defense Information Systems Agency (DISA) for matters related to Circuit provisioning and Authorized Service Interruption (ASI) processing. Contractor shall prepare request for service circuit actions and forward to DISA via the DISA circuit procurement process. Contractor shall track DHA circuit requests through DISA procurement stages (e.g. Telecommunication Service Request, Telecommunication Service Order, and Status of Acquisition Message).

The Contractor shall be responsible for tracking all DHA enterprise IT data circuits both commercial and DISA Managed. The Contractor shall report and track all aspects of the circuit provisioning life cycle. The contractor shall develop a life cycle program for all managed circuits within the MHS and Customers, which outlines the DHA circuit support strategy and ensures the proactive provisioning and management of circuits to Customers. The Contractor shall provide in-depth and continuous tracking of circuits that have been discontinued and that are being discontinued. Contractor shall be responsible for the validity and accuracy of circuit tracking.

The Contractor shall ensure adherence of naming and addressing of all Equipment based on schema approved by Government and documented in the SMM. Contractor shall manage all

changes on circuit assets within the Change Enablement practice, as documented in the SMM. Contractor shall maintain information about all network elements under management in the EITSI provided Asset and Configuration Management system and the CMDB.

The Contractor shall coordinate DISA ASI messages with MTFs, including receipt, review, and work. Designated Contractor Personnel shall distribute ASI messages which may be required to be transmitted via SIPRNet. The Contractor shall process ASI notifications on when a circuit or network will be down. The Contractor shall generate classified material, e-mail and documents concerning the ASI information as required. Contractor shall appropriately secure information where the ASI or the circuit end-points contain classified information.

The Contractor shall monitor, reconcile, and validate the DISA invoice report to ensure correct billing and accuracy, to include all MHS circuits. Contractor shall provide a dashboard on a weekly basis that shows the key activities of Circuit Management for Government review and decision making.

5.7.2 Global Operations Center

The Contractor shall work through the Global Network Operations Center (GNOC) to control all factors involved in the uninterrupted operations of healthcare information technology for all DHA enterprise systems and all MHS network operations, so that they are fully available, secure, and operational. As part of the GNOC, Contractor shall provide command and control on activities occurring in the environment for data network operations.

The Contractor shall participate in the continuous proactive monitoring of the MHS infrastructure on a 24x7x365 basis. At all times, Contractor shall report to and align their GNOC activities with the Government provided Battle Captain and Watch Officer.

The Contractor shall escalate activities to higher tiers of command where appropriate for increased management oversight and decision making.

The Contractor shall provide Major Incident Management to align with and support the EITSI provided practices of Incident Management and Major Incident Management. Contractor shall support and participate in the EITSI provided practices for Problem Management and RCA. The Contractor shall facilitate and document Problem Management and Incident Management troubleshooting meetings, and participate in other meetings as applicable or directed by the Government.

The Contractor shall document and adhere to the policies, processes, procedures, and SOPs of the GNOC within the SMM. Contractor shall participate in the EITSI provided Continual Improvement practice for the evolution and maturity of the GNOC processes and SOPs.

The Contractor shall participate in and support all EITSI practices for the Integrated Environment, including but not limited to: Strategy Management, Availability Management, Capacity Management, Asset and Configuration Management, and Service Level Management.

The Contractor shall align and support the EITSI operations of the Global Service Center and other Customer Interfaces. Where appropriate, Contractor shall serve as tier-2 support for network operations. Contractor shall proactively monitor service interruptions and report major outages in accordance with the EITSI provided Incident Management practices.

The Contractor shall participate in advocating the capabilities and role of the GNOC to all Customers and Mission Partners.

The Contractor shall monitor Release Management activities for supported information systems in order to accurately conduct Event, Incident, and Problem Management and prepare for increases in incident volume. The Contractor shall adjust workflow, processes, and tools as required to proactively respond to shifts in incident or service request volume.

The Contractor shall provide recommendations for monitoring dashboards and improvements to monitoring tools and processes utilizing the EITSI practice for Continual Improvement. The Contractor shall support and implement Continual Improvement initiatives led by the EITSI and as directed by the Government. On an annual basis, Contractor shall provide a report to Government on the effectiveness of the deployed tools and processes.

The Contractor shall work with the EITSI to provide liaison over to Cyber Security Operations such that Cyber Security Events and Incidents are seamlessly worked toward swift resolution.

The Contractor shall provide shift turn-over procedures. Contractor shall conduct formal meetings for the turn-over of shift responsibilities between Contractor Personnel.

5.7.3 Performance Monitoring and Management

The Contractor shall manage and provide for the proactive monitoring of the health of all MHS enterprise IT systems and services to include the underlying core wide area network and local area network infrastructure. Contractor shall execute the process that monitors for the occurrence of events and appropriately action and escalate exception conditions. Contractor shall receive and handle Events generated from other sources, as directed by the Government.

The Contractor shall provide a process and mechanism for implementing monitoring with other programs of record and other vendor services.

The Contractor shall work with the EITSI, the Service Providers and other vendors to implement monitoring for the systems and applications as directed by the Government. The Government will have administrative instructions that direct systems and applications to register their monitoring with the Contractor's Performance Monitoring and Management function. Contractor shall take appropriate action to ensure no event is lost or ignored. Contractor shall manage and record all events in an event log, and manage such logs as prescribed by the SMM.

The Contractor shall work with EITSI to assist in processing unassigned or un-assignable application and infrastructure events and breached thresholds. Contractor shall participate in joint coordination meetings to address Events. Contractor shall track trends that highlight underlying production issues, emerging risks and responding proactively to potential areas of weakness or concern.

The Contractor shall provide proactive alarms and automated incident creation in accordance with thresholds defined in the SMM. Contractor shall ensure immediate alarm notification to specified points of contact for events at critical sites and for critical applications.

The Contractor shall provide event correlation between element management systems and network management tools to support resolution of fault conditions.

The Contractor shall provide input to the EITSI managed Event Management and Correlation System. Contractor shall update the Event Management and Correlation System within designated timeframes with the event information (e.g. categories, types, thresholds, defined actions) as defined in the SMM, for the defined services and Configuration Items under management.

The Contractor shall automate and facilitate processes for continued awareness of network, system, application and service performance and behaviors for continued availability. The Contractor shall ensure that processes for monitoring tightly integrates with the Integrated Environment practices provided by the EITSI; including but not limited to: Availability Management, Event Management, Asset and Configuration Management, and Service Level Management.

5.7.4 DHA SIPRNet Environment Sustainment

Work on this task item will be performed in a Secret environment. Prior to task order start, Contractor shall ensure all Contractor Personnel working on this Task item have a DoD Secret clearance. Contractor shall ensure that Secret clearance are maintained for these staff throughout the performance of this Task item. Contractor must also adhere to the credential requirements for access to health networks as described in Part 6 section 6.5 Contractor Access to Med-COI and DHA Networks.

The Contractor shall provide IT operations in the Secret Internet Protocol Router Network (SIPRNet) environment, currently located at the DHHQ, on a 24x7x365 basis. The Contractor shall execute work for this task within a Secret level environment. Contractor shall be responsible for the RMF, and shall maintain the ATO, for IT Operations in this Secret level environment.

The Contractor shall provide customer support functions including tier-2 helpdesk services, provisioning of tools, and procedures to assist information systems users. The Contractor shall utilize the EITSI managed ITSM tools and processes to deliver customer service, incident management, problem management, resolution, service request management and reporting.

The Contractor shall manage the designated IT assets in the environment, the devices (i.e. network devices, security devices, end-user devices, server, and compute devices) and the software assets and licenses. Contractor will maintain all such IT assets in the EITSI managed CMDB and according to the processes within the SMM, and as approved by the Government.

The Contractor shall utilize, maintain, and update SOPs outlining and describing daily operational tasks. The Contractor shall review and evaluate the SOPs and other documentation relative to the operations support requirements. Contractor shall develop recommendations for changes and improvements in SOPs and other operational procedures through the EITSI managed Continual Improvement practice. Where SOPs are revised the Contractor shall follow the revised SOPs, following Government approval.

The Contractor shall provide immediate customized, short-term training and education as required to new and existing Customers for the use of the environment.

The Contractor shall support DR and Continuity of Operations solutions for mission critical NIPR and SIPRNet systems. Contractor shall support and facilitate changes to the DR and Continuity of Operations as directed by the Government.

5.7.4.1 SIPRNet Workstation Support Services

The Contractor shall maintain the environment and all workstation infrastructure components to include: creating workstation images, deploying workstations to support DHA Personnel throughout National Capital Region, managing workstation and Virtual Desktop Infrastructure, vulnerability patch management of workstations, and tracking of compliance in patching vulnerabilities (e.g. Assured Compliance Assessment Solution, Vulnerability Management Service).

5.7.4.2 Server Infrastructure Support Services.

The Contractor shall manage the infrastructure, applications and systems for the following:

- Server Hardware
- Virtual Server Infrastructure and Application Virtualization
- Windows Infrastructure
- Access Management, Active Directory, Group Policy
- Monitoring and Alerting
- Security Configuration (DISA STIGs)
- Vulnerability Management and Patch Management
- Data Migration & Management for hosted applications
- PKI (CAC and SIPRNet Token)
- Database Management System administration
- Hosted Application Continuity of Operations coordination
- Desktop Virtualization

5.7.4.3 Storage Infrastructure Support Services

The Contractor shall perform storage resource provisioning and management, ensuring compliance with mandatory security configuration requirements (e.g. DISA STIGs). The Contractor shall perform daily incremental and weekly full backups. The Contractor shall manage the infrastructure, applications, and systems for the following:

- Storage Area Network and/or Network Attached Storage configuration and management
- Storage resource provisioning and management
- Backup administration (e.g. disk, tape, other snapshot capability, offsite vaulting)

5.7.4.4 SIPRNet Token Issuance & Administration

The Contractor shall manage the issuance of Alternate Tokens and SIPRNet Tokens for the SIPRNet environment, acting as a Trusted Agent, as directed by the Government.

5.7.4.5 Security Operations Support Services

The Contractor shall perform security operations support services, including the following:

- Certification and Accreditation support
- Assured Compliance Assessment Solution
- Vulnerability Assessment through automated and manual tools
- Vulnerability Management and Reporting
- Host Base Security System administration (either LAN or NWIC)
- Security Information Event Management administration
- Fragmented Orders, Warning Orders, and Information Conditions

Contractor shall respond and comply to with the Joint Task Force-Global Network Operations (JTF-GNO) directives (e.g. Communications Tasking Order) as required.

5.7.4.6 Network Infrastructure Support Services.

The Contractor shall perform network infrastructure support services ensuring compliance with mandatory security requirements, including the following:

- Circuit connectivity and coordination with circuit management
- Core and Boarder Routing Administration
- Core and Access Layer Switch administration
- VPN support for tenant requirements
- Network Management Services
- Authentication Authorization Accounting services (e.g. RADIUS)
- Domain Name System services
- Cable management for data center and workstations
- Network Security and response to Cybersecurity Service Provider
- SIPRNet network encryption and administration of communications security
- Firewall administration
- Virtual Desktop Infrastructure

5.7.4.7 SIPRNet Fiber Alarm Management Support.

The Contractor shall monitor the SIPRNet Fiber Alarm and notify facility security resources when the alarm is sounded. Contractor shall monitor logical alarms and provide physical inspection at least daily.

5.7.4.8 Force Health Protection and Readiness Systems Sustainment

The Contractor shall monitor the current and future FHP&R systems 24x7x365. The FHP&R systems under management are currently Theater Medical Data Store (TMDS) and the Medical Situational Awareness in the Theater (MSAT).

The Contractor shall provide technical support functions for these FHP&R systems, including but not limited to: establishing user accounts, data management, scheduling coordination with the product teams, notifying users of planned and unplanned changes in system availability, and monitoring system performance and demand levels. The Contractor shall provide customer support functions including tier-2 help-desk services, provisioning of tools, and procedures to assist information systems users.

The Contractor shall utilize the EITSI managed SMSs to provide automated management of customer service, request management, incident management, problem management, and reporting for the FHP&R applications. Contractor shall document the processes and procedures for managing and supporting the FHP&R systems in the EITSI provided SMM, as approved by the Government. Contractor shall adhere to the processes in the SMM.

The Contractor shall provide support for both NIPRNet and SIPRNet components of these FHP&R systems. Contractor shall support data transfer and management from the NIPRNet to SIPRNet domains according to Government approved protocols.

5.7.5 Telephony Support Services

The Contractor shall provide Telephony Support Services for design, engineering, business analyst, system integration and tiers 1 thru 3 support tasks. As part of Telephony Support Services, Contractor shall provide direct telephony support and other guidance to the DHA, including those business units that have a 24x7x365 mission. Contractor shall provide core telephony services, such as plain-old-telephone-service (POTS), voice over IP telephone service (VoIP), and advanced ACD functionality. Contractor shall provide ACD flow design for new application support requirements and modifications for existing flows as changes become necessary.

The Contractor shall provide and support a wide range of technologies and disciplines for the support of telephony services; which shall include a number of operating systems, telecommunications carrier and enterprise telecommunications standards and configurations, numerous hardware platforms, data center design, structured cable plant, data network configuration, contact center operations, computer telephony integration, interactive voice response (IVR), solution lifecycle methodology, business continuity, disaster recovery and high-availability.

The Contractor shall routinely coordinate telephony and operational activities with other DHA entities. Contractor shall support remote site integration and continuity of operations declarations and exercises.

The Contractor shall provide the following Telephony support:

- Service Design and Transition Contributions
- IVR logic and verbiage modification
- Skill-based routing creation and modification
- Design, program and optimize initial call handling logic and ongoing tuning
- Configure and manage customized call queues
- Develop and maintain custom programming and processes supporting unique DHA GSC applications
- Site expansion planning, programming and support for data center, new office space and mechanical yard facilities
- Remote and alternate site integration and application extension for virtual contact center deployment and contingency of operations plan capabilities
- RMF Documentation, STIG and IAVM configuration and maintenance
- Security reviews and audit
- Backup of system configurations and call flows
- Ports and Protocol documentation

- Security incident response and reporting
- AD-Hoc Reporting and Analysis
- Server component diagnosis, maintenance and replacement or vendor coordination
- Requirements gathering and translation
- Contact Center Support
- Coordination of telecommunications and other vendors for site surveys and installations
- Coordination of telecommunications and other vendors for hardware and service delivery
- Troubleshooting of handsets and voice stations
- Moves/Adds/Changes coordination and programming
- Support evolving technologies for telephony and the mission of DHA

5.7.6 Service Operations

The task items under 5.7.6 Service Operations require the Contractor to provide services managing Information Systems and devices. DHA intends for this task area to be an exception to its normal practice for acquiring capabilities in the EITS Environment.

5.7.6.1 IT Operations Control

IT Operations Control executes day-to-day tasks related to the operation of infrastructure components and applications. This includes, but is not limited to, System and application monitoring, deployment, testing, sustainment, and routine maintenance.

Contractor shall provide administration and technical operation of Information Systems (e.g. servers, midrange systems, appliances, end-user devices) identified by the Government.

Systems Hosting Management activities shall include, but are not limited to:

- System administration
- Database administration
- Backup and restoration
- Batch, job scheduling and management
- Application monitoring and deployment

5.7.6.2 Systems Management

Systems Management encompasses the management of Information Systems and devices such that they are reliably available and capable of meeting their intended function to serve the mission of the DHA users.

Contractor shall provide management of Systems as identified by the Government. Contractor shall provide for distribution, setup and monitoring of equipment and users. Contractor shall maintain Systems to include upgrades, replacements, and security.

Contractor shall monitor Systems and related devices to ensure their availability and smooth operation.

Systems Hosting Management activities shall include, but are not limited to:

- Software and hardware licenses
- Physical and virtual system instances
- System images for deployment and restoration
- Storage management and allocation
- Security policy application and controls
- Other application and operating system deployment and provisioning
- System patching, upgrades, and fixes
- Multiple operating systems

5.7.6.3 Systems Hosting Management

Systems Hosting Management encompasses the management of devices dedicated to a particular application or operating system. Such hosting devices may be either virtually or physically hosting such application or operating system. Systems Hosting Management prepares, manages, and maintains the machine for such hosting such that it is reliably available and capable of meeting its intended function to serve the mission of DHA users.

Contractor shall manage hosted applications or Systems on existing platforms as identified by the Government in Government identified facilities. Hosting will be either virtually or physically, and either on-site or off-site, as directed by the Government. Contractor shall work with the DAD IO/J-6 as directed for the on-boarding of Customer applications and Systems.

Systems Hosting Management activities shall include, but are not limited to:

- Infrastructure for the hosting platform
- Disk and storage infrastructure
- Data center mechanical space for hosting (i.e. racks and cabinets)
- Network connectivity to hosted systems
- Hypervisor for coordination and management of virtual hosting
- Physical security and controls for hosted systems
- Hosted systems setup and install
- Image management for hosted systems
- Authentication of users to access systems
- Monitoring of hosted system performance and availability

5.8 4ENO Transition

The Contractor shall assist in the coordination and execution of migrating common use IT assets and services to DISA. The DHA is scheduled to move its service desk activities to DISA's Defense Enclave Service (DES) contract. The Contractor shall coordinate with all

DAD IO/J-6 entities, Mission Partners, Service Providers and DISA to begin work to facilitate this move to ensure a successful migration to DES.

5.8.1 Decommission Legacy Shared Services

The Contractor shall assist and coordinate with the Government on which DHA legacy services will be decommissioned. This includes but is not limited to: Communication and Transport Services, Work Station Management, Hosting and Cloud Support Services, Metro Network Management, Identity/Access Management and Enterprise Management, Global Service Center, and Web Development. The Contractor shall coordinate these activities through an Integrated Master Schedule and will work with Cyber Security Division and the DHA Authorizing Official to decommission legacy systems.

5.8.2 ITSM Tools Transfer

The Contractor shall assist and coordinate with the Government to determine how to migrate the DHA ITSM Tools to DISA's DES. The DHA will be fully migrated to a FEDRAMP IL4 cloud based solution. The Contractor shall coordinate with DISA on behalf of the DHA to migrate to a DISA provided ITSM Tool. The Contractor shall execute appropriate actions to migrate the data and then decommission cloud instances as required.

5.8.3 Knowledge Transfer

The Contractor shall coordinate and execute knowledge management transfer to the DISA DES to ensure DHA customers and the MHS continue to receive uninterrupted support. The Contractor shall assist with new documentation spanning all SMS tools, processes, and procedures as required for a successful transition of services.

5.8.4 Migration Activities

The Contractor shall develop an Integrated Master Schedule to track and coordinate all activities, coordinate all migration activities from DHA shared services, and shall create a dashboard for reporting.

The Contractor shall plan, coordinate, and execute all migration activities from DHA Shared Services to include but not limited to: Communication and Transport Services, Work Station Management, Hosting and Cloud Support Services, Metro Network Management, Identity/Access Management and Enterprise Management, Global Service Center, and Web Development.

5.8.5 Post Migration Environment Cleanup

The Contractor shall perform post migration cleanup as necessary for all DISA DES services; these include but are not limited to multiple legacy servers, circuits, stale objects within Identity Management, and legacy tools. The Contractor shall perform an inventory of all legacy service infrastructure components and coordinate with DISA DES to ensure the new environment is as efficient and accurate.

5.8.6 Test and Validation Activities

The Contractor shall perform testing to ensure that migration solutions meet technical requirements, customer expectations, and verifies IT operations are able to support the migration as implemented.

5.8.7 Transition Communications

The Contractor shall coordinate in the administration of all communications between the DHA and DISA. The Contractor shall create a communication plan and awareness campaign for all authorized users, customers, and mission partners to ensure continuity within the MHS for anything required to migrate to DISA DES services.

5.8.8 Transition Coordination

The Contractor shall work with the Government to coordinate the transition of DHA moving to DISA DES Services. The Contractor shall produce any required documentation necessary to ease the migration to DISA DES services.

5.8.9 Transition Program Management

The Contractor shall perform all program and project management tasks required to migrate legacy DHA services to DISA DES. This should be viewed as complex program with multiple projects and initiatives that need to be accomplished in a sequential and logical technical order. The Contractor shall plan and coordinate the resources to migrate; and to ensure issues and risks are managed. The Contractor shall align migration projects to requirements and deliver projects from request through end solution, including turnover to customers and validation that project requirements were met.

5.8.10 Transition SLAs

The Contractor shall assist and coordinate with the Government changeover of any existing performance standards (e.g. Customer SLAs, Memorandum of Understanding, and Memorandum of Agreement) that the DHA has with its Customers and Mission Partners to DISA where necessary. The Contractor shall review existing SLAs and recommend to the Government a plan to modify or migrate SLAs or create new SLAs as necessary. This will require reviewing the exiting DHA portfolio of agreements with Customers and coordinating changes in performance standards as necessary.

PART 6
6.0 INFORMATION TECHNOLOGY & SECURITY

6.1 Contract Work Classification

Certain work under this contract is SECRET. Contractor Personnel shall undergo a Tier 1 (T1) investigation or higher. Contractor Personnel must obtain favorable suitability adjudication prior to commencement of duties and maintain favorable suitability adjudication.

Contractor shall follow the DHA Personnel Security Office guidelines for submittal of security clearances. Contact the DHA Personnel Security Office for guidance on the appropriate background investigation required for personnel on the contract.

Contractor shall initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to Controlled Unclassified Information (CUI).

Contractor shall initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to MHS Sensitive Information.

6.1.1 Security Clearances

Security Clearances may be required for certain Labor Categories. Labor categories requiring Secret Clearance will be identified in Attachment 4 (Special Clearance and Certification Requirements).

6.2 Automated Data Processing / Information Technology Levels

Contractor Personnel shall comply with the requirements of the DoD 8140.01 for baseline certifications.

Automated Data Processing/Information Technology (ADP/IT) levels and position sensitivity designation for positions under this BPA and any Call Orders are defined in Attachment 4 (Special Clearance and Certification Requirements).

Contractor shall follow the DHA Privacy Office guidelines for submittal of Information Technology security clearances and ensure all Contractor Personnel are designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of the position sensitivity designations. Contact the DHA Privacy Office for guidance on the appropriate ADP/IT level of certification for all Contractor Personnel.

Immediately report to the DHA Privacy Office and deny access to any automated information system, network, or MHS Sensitive Information if a Contractor Personnel filling a sensitive position receives an unfavorable adjudication, if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the appropriate government representative for security reasons.

6.2.1 ADP/IT I

Critical sensitive position. These are positions where the individual is responsible for the development and administration of Military Health System Information System (MHS IS)/network security programs and has the direction and control of risk analysis and/or threat assessment.

6.2.2 ADP/IT II

Non-critical sensitive position. These are positions where an individual is responsible for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADT/IT I category.

6.2.3 ADP/IT III

Critical sensitive position.

6.3 PII/PHI, and Federal Information Requirements

Contractor shall comply with Federal Information Requirements for Personally Identifiable Information (PII) and Public Health Information (PHI). (Refer to Clause Section for DHA Procedures, Guidance, and Information 224.90 as applicable).

6.4 Cyber Security Training

Contractor Personnel and associated subcontractor personnel performing cybersecurity / cyberspace functions shall comply with the requirements in Exhibit 5.3 (Labor Role Descriptions) and Attachment 4 (Special Clearance and Certification Requirements).

6.4.1 Contractor Personnel Cybersecurity Information Assurance Training

All Contractor Personnel and associated subcontractor personnel working Cybersecurity Information Assurance / Cyberspace functions must comply with DoD training requirements in Department of Defense Directive (DoDD) 8140.01 and DoD 8570.01-M.

6.4.2 Information Assurance Certification

All Contractor Personnel and associated subcontractor personnel working Cybersecurity Information Assurance shall have the proper and current Information Assurance certifications to perform Information Assurance functions, in accordance with DoD 8570.01–M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable Information Assurance certification requirements, including: DoDD 8140.01 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.239-7001. The baseline certification as stipulated in DoD 8570.01-M must be completed prior to the Contractor Personnel assuming their roles in providing Contractor Services.

6.4.2.1 Documentation of Information Assurance Certification

Upon request by the Government, the Contractor shall provide documentation supporting the Information Assurance certification status of Contractor Personnel performing Information Assurance functions as part of Contractor Services.

6.4.3 Acceptable Use of IT Resources

All Contractor Personnel that require access to Defense Health Agency Information Technology (DHA IT) must comply with the requirements of DHA-PI 8140.01, Acceptable Use of Defense Health Agency IT, to include those Contractor Personnel with privileged access.

6.5 Contractor Access to Med-COI and DHA Network(s)

Contractor FSO/Security POC shall notify the DHA Personnel Security Office after being awarded a contract that requires access to a DoD system. Contractor Personnel requiring access to the HA/DHA networks for performance of their tasks require a background investigation and the security awareness training. The Contractor shall be prepared for this process as it could take two (2) or more weeks. The Facilities Security Officer/Security POC shall submit a Standard Form (SF) either a SF85 or SF86 as appropriate to DHA's Personnel Security Office for a background investigation for each contractor worker that does not currently have the required security clearance.

6.5.1 SF-85/86 Notifications

Contractor's FSO/Security POC must notify the Personnel Security Office when the contractor has submitted the SF-85/86. The FSO/Security POC, or the COR must notify the DHA Personnel Security Office in writing of a contractor's termination from the contract, including the termination date.

6.5.2 Credentials for Accessing SIPRNet

To be provided.

6.6 General Cybersecurity Requirements – Information Systems

Contractor information system shall be subject to the security requirements in:

- DHA Administrative Instruction 042, “Security of Unclassified DoD Information on non-TMA Information Systems”,
- DoDI 8582.01, “Security of Unclassified DoD Information on non-DoD Information Systems”, and
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (available at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time of the assumption of services or as authorized by the Contracting Officer.

The Contractor shall comply with cybersecurity requirements of DHA-IPM 18-015 https://health.mil/Reference-Center/Policies Cybersecurity Program Management).

Contractor Personnel must take the DoD Cyber Awareness Challenge utilize the Defense Health Agency (DHA) Learning Management System, Joint Knowledge Online (JKO).

6.6.1 SAR Certification of Compliance

The Contractor SSO shall annually self-certify that the Contractor owned Information System and facilities are compliant with the applicable NIST security controls, by submission of a Security Assessment Report (SAR) and security test plan for compliance of testing security controls.

6.6.2 NIST SP 800-171 Compliance

The Contractor shall implement NIST SP 800-171, prior to the award of the contract.

6.6.3 NIST SP 800-171 Variance

The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO). The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be non-applicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

If the DoD CIO has previously adjudicated the Contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting such recognition under this contract.

6.6.4 FedRAMP for External Cloud Services

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (www.fedramp.gov) and that the cloud service provider complies with requirements in paragraphs 6.5.6 through 6.5.10 for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

6.6.5 Cyber Incident Reporting

When the Contractor discovers a cyber incident that affects a covered Contractor information system or the covered defense information residing therein, or that affects the Contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall conduct a review and report the incident.

6.6.5.1 Cyber Incident Review

Contractor shall conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor

information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support.

6.6.5.2 Cyber Incident Report

Contractor shall rapidly report cyber incidents to DoD at https://dibnet.dod.mil/portal/intranet/. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil/portal/intranet/.

6.6.5.3 Medium assurance certificate

In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/.

6.6.5.4 Cyber Incident Management

The Contractor shall comply with the incident management requirements of Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program".

6.6.6 Malicious Software

When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, Contractor shall, complying with instruction of the DoD Cyber Crime Center (DC3), submit the malicious software to DoD Cyber Crime Center (DC3), in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer or any other entity or individual, without the specific, explicit instruction, of the Contracting Officer. Care must be taken to prevent malicious software from causing damage.

6.6.7 Media preservation and protection

When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems and all relevant monitoring/packet capture data for at least ninety (90) days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

6.6.8 Access for Forensic Analysis

Contractor shall facilitate access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

6.6.9 Cyber incident damage assessment activities

If DoD elects to conduct a damage assessment, Contractor shall provide all of the damage assessment information gathered, as requested by the Contracting Officer.

6.6.10 Hosting DoD Information in a Non-DoD Information System

Contractor shall apply other information systems security measures when the Contractor reasonably determines that information systems security measures may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., HIPAA) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan. The Contractor must submit the system security plan within 5 Business Days upon the CO request.

6.6.11 Data Location

The Contractor shall maintain within the United States or US territories all Government data that is not physically located on DoD premises, unless the Contractor receives written direction or approval from the Contracting Officer to use another location, in accordance with DFARS 239.7602-2(a).

6.7 Risk Management Framework (RMF) for DoD IT

Contractor shall ensure that all Information Systems (IS), Platform Information Technology (PIT) and the Integrated Services or Products utilized by Contractor for Contractor Services, that receive, transmit, store, or process nonpublic government data are accredited in accordance with DoD Instruction (DoDI) 8510.01, RMF for DoD IT and comply with annual Federal Information Security Management Act (FISMA) security control testing. IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253, implement a corresponding set of security controls from the NIST SP 800-53, and use assessment procedures from NIST SP 800-53A with additional DoD-specific assignment values, overlays, implementation guidance, and assessment procedures as required.

All Contractor systems subject to RMF must present evidence of authorization in the System Security Plan, SAR Plan of Action and Milestones (POA&M) and authorization decision document or show that the system has a DoD RMF or equivalent DoD Component PIT system accreditation decision that is current within 3 years within 5 Business Days of CO request. Evidence of FISMA compliance must be presented in the form of a POAM. Contractor systems utilized for Contractor Services must have and maintain an Authority to Operate (ATO) by contract award.

The Contractor shall implement security controls in accordance with NIST implementation and validation requirements specified in the NIST SP 800-37 RMF.

The Contractor shall configure the information system in accordance with Defense Information System Agency (DISA) Security Requirements Guides (SRGs) and security technical implementation guides (STIGs).

The Contractor shall ensure that the information system conforms to the requirements of DoDI 8551.01 “Ports, Protocols, and Services Management (PPSM)”.

The Contractor shall ensure that the information system shall authenticate all entities as specified in DoDI 8520.03 “Identity Authentication for Information Systems” prior to granting access.

The Contractor shall Public Key enable the information system, implementing digital signature and encryption requirements specified in DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling."

Contractor shall be responsible for compliance with the United States Cyber Command issuances and Information Assurance Vulnerability Management (IAVM) issuances by ensuring that the issuances are assessed, implemented, and maintained throughout development and sustainment in accordance with specified timelines.

The Contractor shall support reciprocity, by providing all NIST security documents directed information to the government.

The Contractor shall implement system level protection and detection capabilities that are consistent with their contract for NIST Security requirements that meet DoD and DHA Cybersecurity Architectures.

Information security continuous monitoring (ISCM) is maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a critical part of the risk management process to ensure that IS and PIT operations remain within an acceptable level of risk despite any changes that occur. The Contractor shall maintain ongoing monitoring, analysis and incident response procedures for all IS and PIT systems under this requirement in accordance with NIST SP 800-137.

6.8 Commercial Cloud Computing Services

Contractors contracting for external IT services in the form of commercial cloud computing services must comply with DoD cloud computing policy and procedural guidance as published in DoD Cloud Computing Security Requirements Guide current version.

To the maximum extent practicable, cloud computing services that are commercial items shall be acquired under the terms and conditions (e.g., license agreements, End User License Agreements (EULA), Terms of Service (TOS), or other similar legal instruments or agreements) customarily provided to the public, to the extent that such terms and conditions are consistent with Federal law and otherwise satisfy the Government's needs, including those requirements specified in this section. Any applicable service provider terms and conditions shall be incorporated into the contract (e.g., by attachment or other appropriate mechanism).

Any contract awarded to acquire cloud computing services from any cloud service provider (e.g., contractor or subcontractor, regardless of tier), must have been granted authorization to provide the relevant cloud computing services in accordance with the Cloud Computing SRG (version in effect at time of contract award) found at https://public.cyber.mil/. All necessary SRG requirements, including cloud access point connections and authorizations to operate, must be satisfied before the cloud computing service becomes operational.

Contractors contracting for Cloud services will only use cloud services that have been issued both a DoD Provisional Authorization by DISA and obtained an Authority to Operate (ATO) (Reference (f)) by the DHA Authorizing Official.

Non-DoD cloud services hosting CUI (Personally Identifiable Information (PII)) shall be connected to customers through a Cloud Access Point that has been approved by the DoD CIO and have a Cyber Security Service Provider.

Cloud Service providers shall establish a security baseline in accordance with the Federal Risk Authorization and Management Program (FedRAMP) and achieve a FedRAMP (level 4-5) authorization to store/process DoD sensitive information within the Cloud Service Provider and be compliant with DoD Cloud Computing Security Requirements Guide current version.

The contractor shall connect to customers through a DoD Cloud Access Point (CAP) for commercial cloud services hosting CUI and comply with DoD Cloud Computing SRG current version.

The contractor shall implement DoD Cloud Computing SRG current version specific security requirements for cloud services that contain PII/Protected Health Information (PHI).

The contractor is solely responsible for the cost associated with obtaining a FedRAMP Provisional Authorization to host Federal Government missions and obtaining a DoD Provisional Authorization to Operate (P-ATO).

The Contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing SRG, (version in effect at the time of contract award) found at https://public.cyber.mil/.

PART 7
7.0 ATTACHMENTS AND EXHIBIT LISTING

Highlighted items are included as part of September 9, 2020, release to Industry.

BPA PWS, Attachments and Exhibits

The following documents are part of the BPA PWS.

PWS	Blanket Purchase Agreement (BPA) Performance Work Statement
Attachment 1	Definitions and Acronyms
Exhibit 1.2	Operating Level Agreement Outline
Exhibit 3.4	Severity Levels
Exhibit 5.3	Labor Role Descriptions
DD Form 254	Contract Security Classification Specification

Call Order PWS, Attachments and Exhibits

For reference, the following are documents that are expected to be part of any Call Order PWS.

PWS	Call Order Performance Work Statement
Attachment 4	Special Clearance and Certifications
Attachment 5	Facilities Receiving Services
Attachment 8	Government Provided Workspace
Exhibit 2.1	Milestone Deliverables
Exhibit 3	Performance Requirements Summary
Exhibit 3.1	Service Level Matrix
Exhibit 3.2	Service Level Definitions
Exhibit 3.3	Reports Matrix

7.1 Forms

The following forms are to be completed by the FSO/Security POC, or COR once the Contractor is granted the proper background investigation.

7.1.1 Contractor CAC Request Process

Will be provided upon issuance of award.

7.1.2 DHA Contractor Onboarding Requirements.

Will be provided upon issuance of award.

7.1.3 DHA Contractor Training Instructions.

Will be provided upon issuance of award.

7.1.4 Contractor Personnel List

This provides the required fields and form for the All Personnel Report.

7.2 Attachments

These Attachments are appended to the PWS.

Document Number	Document Name	BPA Call Order
Attachment 1	Definitions and Acronyms	BPA
Attachment 1 (Definitions and Acronyms) provides definitions for terms and acronyms used in the BPA PWS and Call Order PWS. **Filename:** DRAFT MHS EITSI Attachment 1 – Definitions 0.2 200806.docx		
Attachment 4	Special Clearance and Certifications	Call Order
Attachment 4 (Special Clearance and Certifications) identifies the specific skills, clearances and certifications that are required for certain Contractor Personnel roles. **Filename:** DRAFT MHS EITSI Attachment 4 – Special Clearance and Certifications 0.1D 200616.docx		
Attachment 5	Facilities Receiving Services	Call Order
Attachment 5 (Facilities Receiving Services) identifies the Customers' facilities receiving services from the Global Service Center and the DAD IO/J-6. **Filename:** DRAFT MHS EITSI Attachment 5 – Facilities Receiving Services 0.1D 20mmdd.xlsx		

Document Number	Document Name	BPA Call Order
Attachment 8	Government Provided Workspace	Call Order
Attachment 8 (Government Provided Workspace) identifies the space (e.g. cubicles, offices, desks) in Government facilities for Contractor work that the DAD IO/J-6 has identified for Contractor usage in providing Contractor Services. **Filename:** DRAFT MHS EITSI Attachment 8 – Government Provided Workspace 0.1 20mmdd.xlsx		

7.3 Exhibits

These Exhibits are documents attached to the PWS and establishes requirements.

Document Number	Document Name	BPA Call Order
Exhibit 1.2	Operating Level Agreement Outline	BPA
Exhibit 1.2 (Operating Level Agreement Outline) outlines the required elements of OLAs to be signed between the Integrated Service Providers. **Filename:** DRAFT MHS EITSI Exhibit 1.2 – OLA Outline 0.1 200902.docx		
Exhibit 2.1	Milestone Deliverables	Call Order
Exhibit 2.1 (Milestone Deliverables) describes the milestones to be achieved and provided as deliverables as part of Contractor Services. **Filename:** DRAFT MHS EITSI Exhibit 2.1 – Milestone Deliverables 0.1 20mmdd.xlsx		
Exhibit 3	Performance Requirements Summary	Call Order
Exhibit 3 (Performance Requirements Summary) describes the performance standards and AQLs for the tasks and deliverables required by the Call Order. The Government will reference the information in the PRS when conducting surveillance of contractor performance and determining incentives or remedies. **Filename:** DRAFT MHS EITSI Exhibit 3 – Performance Requirements Summary 0.1 20mmdd.docx		

Document Number	Document Name	BPA Call Order
Exhibit 3.1	Service Level Matrix	Call Order
Exhibit 3.1 (Service Level Matrix) lists individual service level measures to be reported and achieved in a simple matrix along with any applicable performance incentives. **Filename:** DRAFT MHS EITSI Exhibit 3.1 – Service Level Matrix 0.1 206016.xlsx		
Exhibit 3.2	Service Level Definitions	Call Order
Exhibit 3.2 (Service Level Definitions) provides details on the individual service level measures to be achieved, as listed in Exhibit 3.1 (Service Level Matrix). **Filename:** DRAFT MHS EITSI Exhibit 3.2 – Service Level Definitions 0.1 200806.docx		
Exhibit 3.3	Reports Matrix	Call Order
Exhibit 3.3 (Reports Matrix) lists the essential report deliverables to be provided as part of Contractor Services. **Filename:** DRAFT MHS EITSI Exhibit 3.3 – Reports Matrix 0.1 200806.xlsx		
Exhibit 3.4	Severity Levels	BPA
Exhibit 3.4 (Severity Levels) describes the scale for how Incidents and Problems shall be rated as to urgency and impact for appropriate actioning and prioritization. **Filename:** DRAFT MHS EITSI Exhibit 3.4 – Severity Levels 0.1D 200806.		
Exhibit 5.3	Labor Role Descriptions	BPA
Exhibit 5.3 (Labor Role Descriptions) lists the required qualifications and duties for the labor roles to be performed by the Contractor as part of Contractor Services. This includes requirements for Key Personnel roles. **Filename:** DRAFT MHS EITSI Exhibit 5.3 – Labor Role Descriptions 0.1 20xxxx.docx		
DD Form 254	Contract Security Classification Specification	Call Order
DD Form 254 Contract Security Classification Specification details the Contractor facility clearance and personnel clearance requirements. **Filename:**		

Document Number	Document Name	BPA Call Order