Performance Work Statement
Defense Manpower Data Center (DMDC) Enterprise
Information Technology Services (EITS) I I
DMDC Enterprise Development Operations (DEVOPS)

Enterprise Development Operations (DEVOPS)
EITS II Task Order
Order ID No: 47QFMA18K0030-0018

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) requires information technology services to support the implementation, configuration and maintenance of an Enterprise Development Operations (DEVOPS) infrastructure and supporting processes for the DMDC Enterprise Development Environments to be located in DMDC's enterprise software hosting environment.

2.0 BACKGROUND

Development Operations (DEVOPS), henceforth referred to as DevSecOps, emphasizing the importance of security within the domain, is the collaboration, integration and communication of both software developers and other IT Professionals focused on the automation of software delivery and infrastructure changes to deliver business capabilities in a manner that reduces cost and increases business value. The adoption of this methodology is supported and enforced through the implementation of automation tools that will increase standardization and dependability when integrated as a unified system.

With the higher adoption of the Agile Software Development methodology and the strain of reduced budgets within the Department of Defense, DMDC needs to ensure timely delivery of defect free code to its production environment while reducing the dependency on touch labor to realize this increased productivity level. This is compounded with the need to ensure security standards are enforced and auditability is maintained without sacrificing that agility. The new DMDC DevSecOps environment will be an integrated ecosystem comprised of continuous deployment; continuous integration and continuous quality assurance in order to affect application release and infrastructure build automation accomplishing a complete end-to-end continuous delivery mechanism.

3.0 SCOPE

The Contractor shall provide the personnel and management necessary to enable DMDC to implement and maintain the processes and environment to produce an optimized Enterprise DevSecOps Environment utilizing Government Furnished Equipment and Software. This will also require constant coordination with the Service Delivery (SD) and Technical Services (TS) Directorates in order to facilitate workload changes into the toolset pipeline.

4.0 REQUIREMENTS. *The Contractor shall support:*

4.1 CONTINUOUS INTEGRATION INFRASTRUCTURE

4.1.1 Sustain and enhance the Enterprise Continuous Integration Infrastructure and its related process workflows to support DMDC Continuous Integration. All requirements, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of, and be approved by, the DMDC

Architecture Review Board before implementation by the contractor will be authorized. This shall include the sustainment and enhancement of the:

4.1.1.1 Scalable Continuous Integration orchestration infrastructure in the DMDC Enterprise Development and Testing Environments utilizing the Government provided tools. Enhancements shall include configuration and maintenance of Architecture Review Board (ARB) approved technologies and architectures for container orchestration.

4.1.1.2 Software configuration management system in the DMDC Enterprise Development and Testing Environments.

4.1.1.3 Integrated source code repository, which is capable of providing version control for multiple coding languages and platforms (Java, .Net, JavaScript, Ruby, Python and others as identified), utilized for the consolidation of all DMDC source code repositories.

4.1.1.4 Integrated build automation tool and repository, which is capable of providing on-demand and triggered automation tasking for continuous integration activities to be utilized as the centralized DMDC build automation repository for DMDC developed applications.

4.1.1.5 Job automation templates, utilizing the Government provided toolsets that enable on-demand, unattended application builds and deployments of DMDC developed applications through all build, test and production environments to their authorized containers segments as designated in the Configuration Management Repository.

4.1.1.6 Job automation templates, utilizing the Government provided Jenkins Template Toolset that will enable on-demand, unattended database schema builds and deployments through all build, test and production environments to their authorized multi-tenet database segments as designated in the Configuration Management Repository.

4.1.1.7 Process workflows and orchestration engine that enable the on-demand automation of Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) compliant creation and configuration of virtual workstations and servers, network instantiation, application build, test and release, as well as registering all required Configuration Item attributes into the Central Configuration Repository.

4.1.1.8 Process workflows and orchestration engine automation, utilizing the Government provided Information Technology Service Management (ITSM) workflow management toolset, that will automate Continuous Integration tasks (build, test and deploy) based on request, issue tracking and resolution events in the centralized Change Management Database (CMDB).

4.1.1.9 Automated verification and update of all configuration management attributes for application and database deployments and changes in the Government provided central configuration management repository.

4.1.1.10 Automated verification and update of all dependency attributes (software libraries) for application and database deployments and changes in the Government provided central configuration management repository.

4.1.1.11 Process and procedures that enable DMDC software developers to commit code changes to the repository daily for insertion into the Continuous Integration workflow.

4.1.1.12 Processes for automating the download of DMDC approved commercial software code libraries from only DMDC approved code sources upon request submitted through the Change Request

system.

4.1.1.13 Automated procedures, workflows, form wireframes scripting and dashboards to be implemented through the ITSM workflow management toolset to allow for visibility and auditing of each step in the Continuous Integration process flow.

4.1.1.14 Architecture, analysis, design, and maintenance documentation for executing Continuous Integration processes and procedures, and update of the associated artifacts within 10 business days of change.

4.2 CONTINUOUS DEPLOYMENT TESTING INFRASTRUCTURE

4.2.1 Sustain and enhance the Enterprise Continuous Deployment Testing Infrastructure and its related process workflows to support DMDC Continuous Deployment Testing. All recommendations, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board. This shall include:

4.2.1.1 Sustainment and enhancement of the process workflows to enable the automation of the Government provided Quality Assurance tools Redwood HQ, SOAPUI, Selenium and Junit throughout the Software Development Lifecycle (SDLC) process to allow developers access in any phase of deployment.

4.2.1.2 Sustainment and enhancement of the core functional testing capabilities in the automated Continuous Integration process by utilizing pre-defined Quality Assurance Test Cases to be provided by the Government Quality Assurance (QA) staff.

4.2.1.3 Sustainment and enhancement of the centralized dashboard that analyzes data captured in the DMDC Enterprise Continuous Deployment Testing infrastructure that will register bugs or issues in a central issue tracking repository, email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific details.

4.2.1.4 Architecture, analysis, design, and maintenance documentation for executing continuous integration test cases, and update the associated artifacts within 10 business days of change.

4.3 APPLICATION SECURITY TESTING INFRASTRUCTURE

4.3.1 Sustainment and enhancement of the Enterprise Continuous Application Security Testing Infrastructure and its related process workflows as a recommendation for implementation in DMDC's enterprise software hosting environment to support DMDC Continuous Application Security Testing. All recommendations, plans, process workflows and required system specifications shall be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review. This shall include sustainment and enhancement of the:

4.3.1.1 Government provided security testing tools, Sonatype (library compliance), Fortify (static code analyzer) and WebInspect (dynamic code analyzer) in order to provide automated, and on-demand through ITSM workflow automation toolset, application security testing to meet the requirements under the Enclave and Developers Security Technical Implementation Guide (STIG).

4.3.1.2 Centralized dashboard that analyzes data captured in the DMDC Enterprise Application Security Testing infrastructure that will email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific security details.

4.3.1.3 Provide architecture, analysis, design, and maintenance documentation for executing continuous integration test cases, and update the associated artifacts within 10 days of change.

4.4 PERFORMANCE TESTING INFRASTRUCTURE

4.4.1 Sustain and enhance the Enterprise Performance Testing Infrastructure and its related process workflows to support DMDC Application Performance Testing. All recommendations, plans, process workflows and required system specifications will be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board. This shall include sustainment and enhancement of the:

4.4.1.1 Performance testing harness that will provide DMDC application load and stress functionality in an on-demand fashion using the Government provided testing software.

4.4.1.2 Automated performance testing process workflows that will evaluate the responsiveness, speed, scalability and stability characteristics of DMDC applications. Leverage applicable test case scenarios currently supported by the development and QA teams as applicable.

4.4.1.3 Automated load testing process workflows that will constantly and steadily increase the load on the identified system until the time it reaches the threshold limit. The goals of load testing are to expose the defects in application related to buffer overflow, memory leaks and mismanagement of memory. Another target of load testing is to determine the upper limit of all the components of application like database, hardware and network etc.

4.4.1.4 Automated stress testing process workflows that will evaluate the applications behavior beyond normal or peak load conditions. Test the functionality of the application under high loads.

4.4.1.5 Centralized dashboard that analyzes data captured in the DMDC Enterprise Performance Testing infrastructure that will email alerts upon discovery of an issue or failure, allow for creation of customizable reports and provide application specific performance details.

4.4.1.6 Architecture, analysis, design, and maintenance documentation for executing Application Performance Testing, and update the associated artifacts within 10 business days of change.

4.5 PROVIDE APPLICATION MONITORING SUPPORT

4.5.1 Working with IT Operations (ITOps), support shall be provided to ensure monitoring of the DevSecOps infrastructure can be adequately performed. This will require regular interaction with ITOps and the tools used to perform monitoring tasks.

4.5.2 DevSecOps monitoring shall include (but may not be limited to) monitoring of container infrastructure, container network infrastructure, as well as the build and deployment systems.

4.5.3 Any monitoring components installed within the DevSecOps infrastructure shall integrate with enterprise monitoring implementations. Sustainment of this infrastructure must be performed during the performance period.

4.6 APPLICATION RESILIENCE TESTING

4.6.1 Sustain and enhance the Enterprise Application Resiliency Testing process workflows as a recommendation for implementation in DMDC's enterprise software hosting environment to support DMDC Application Resilience Testing. All recommendations, plans, process workflows

and required system specifications shall be documented in the DMDC Enterprise Architecture Repository, meet compliance with all applicable standards of and be approved by the DMDC Architecture Review Board before implementation by the contractor will be authorized. Resiliency Testing is defined as the process of subjecting an application or IT system to unforeseen events and documentation of the results of system behavior induced by the event. These events may include a power outage, running out of disk space, network outages, etc. The goal of this testing is to ensure that these unforeseen events do not result in the loss of any data.

4.6.2 Architecture, analysis, design, execution and maintenance documentation for executing the DMDC Resiliency Test Plan, and update the associated artifacts within 10 business days of change.

4.7 (OPTIONAL CLIN)(T&M) DEVSECOPS IMPLEMENTATION SUPPORT FOR TRANSITION TO A NEW PLATFORM/ARCHITECTURE (CLOUD, AWS, MILCLOUD, ETC)

4.7.1 Provide DMDC with best practices, industry knowledge and expertise, and technical support, during and after DevSecOps implementation in DMDC's enterprise software hosting environment. Implementation will be completed within 90 days

4.7.2 Update DevSecOps implementation plan within 5 business days of any changes; develop and monitor implementation schedule and facilitate implementation status meetings.

4.7.3 Perform research to validate that reported defects are defects. Determine root cause of software problems and recommend remediation. Triage defects reported by the customers and assigned a 'priority level'.

4.7.4 Assist in ad hoc reporting and serve as point of contact between product development group and customers.

4.7.5 Provide a monthly report on implementation status reporting and schedule.

5.0 REPORTS AND MEETINGS

Unless specified elsewhere within this PWS, all reports and deliverables shall be submitted in Microsoft Office products to include Microsoft Project and shall be accessible via web. All diagrams shall be delivered in a readable format (PDF or standard formats and hard copy (including oversized diagrams).

5.1 PROGRAM MANAGEMENT PLAN (PMP)

Provide a draft Program Management Plan (PMP) to the COR within 10 business days of award that describes the overall approach to managing the DEVOPS requirements. This PMP shall include the contractors overall management approach, quality control plan, operating procedures, staffing approach, milestones, tasks, subtasks and the overall Work Breakdown Structure (WBS). The PMP shall identify and assign tasks, major milestones, dates and dependencies, and indications of critical path. Tasks from the final Government-approved PMP shall be selected as milestones against which Contractors' progress is monitored. The PMP shall include milestones and measurable indicators that can be used to evaluate satisfactory progress toward delivering services. The Contractor shall include in the PMP: the status, statistics; risk management review; critical path and other milestone progress checks and updates; as well as technical content review. The program plan shall be finalized 45 business days after TO award via deliverables acceptance criteria under PWS Section 5.0 – "Deliverables." The PMP may be updated, after discussions and mutual agreements, as a result of changes in priorities or the receipt and acceptance of new deliverables.

5.2 KICK-OFF MEETING

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the TO and will aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the DMDC COR, and GSA COR within 3 business days.

5.3 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

Prior to the delivery of the monthly SMR, the contractor shall also hold monthly pre-SMR meetings with designated Government representatives for each awarded task order. The purpose of the pre-SMR meeting shall be to present the same documentation that will be presented at the official SMR while also reviewing each task order's specific task order data (listed above). Each contractor task order manager shall coordinate the pre-meeting, distribute the pre-meeting materials and facilitate any changes to the task order's data through the DMDC COR and contractor Program Manager.

5.4 Problem Notification Reports

The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.0 Deliverables

All deliverables and work products shall be submitted to the COR in electronic format for acceptance and approval. The acceptance of deliverables and satisfactory work performance shall be based on the timeliness, accuracy and standards as specified in the requirements of the PWS.

Deliverable	PWS	Delivery Date
Enterprise Continuous Integration System Engineering	4.1.1	Continuous
Enterprise Continuous Deployment Testing System Engineering	4.2.1	Continuous
Enterprise Application Security Testing System Engineering	4.3.1	Continuous
Enterprise Performance Testing System Engineering	4.4.1	Continuous
Enterprise Application Resiliency Testing System Engineering	4.6.1	Continuous
Implementation Support	4.7	Continuous
Update Implementation Plan	4.7.2	Within 5 business days of change
Implementation Status Monthly Report	4.7.5	Monthly

Program Management Plan	5.1	Draft submitted within 10 business days of order award; Final submitted within ten days after receipt of Government comments. Updates as needed and no less frequently than 30 days after exercise of an Option
Post Award Conference	5.2	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
SMR Documentation	5.3	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
Problem Notification Reports	5.4	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ

7.0 QUALITY SURVEILLANCE

The Government may follow the Appendix P - Quality Assurance Surveillance Plan) to EITS II IDIQ Base Contract

8.0 Performance Objective and Thresholds:

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.
Key Personnel: Provide qualified personnel in a timely manner.	New or replacement personnel in place within fourteen (14) calendar days of negotiated date.

8.1 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.

- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

9.0 Contract Administration.

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

9.1 Contract Type: The contract type for this Task Order will be firm fixed price

9.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award with two one-year options.

9.3 PLACE OF PERFORMANCE / HOURS OF OPERATION: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section - Travel.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET (8 a.m. to 5 p.m. PT for contractors located on the West Coast), Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

9.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

9.5 Points of Contact:
DMDC COR will be assigned Post Award

GSA Contracting Officer (CO)
Mr. David Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contract Specialist (CS)
Mr. Raj Singh
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West

Philadelphia, PA 19106
E-mail: rajdeep.singh@gsa.gov
Tel: 215-446-2868

GSA Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Scott.ostrow@gsa.gov
Tel: 215-446-4497

9.6 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Sections 10.8 thru 10.9 of the EITS II Base IDIQ

9.7 Travel: The cost reimbursable not-to-exceed travel limit is estimated at $5,000.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR. All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

9.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

In addition, certain contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances, as directed by the Government. Contractor personnel shall possess these security clearances at Task Order award.

10.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

11.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

Market Research
for
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services (EITS) II

Requirement:
This acquisition was conducted by GSA's Federal Acquisition Service (FAS), Mid-Atlantic Region on behalf of the Defense Manpower Data Center (DMDC) to procure IT services to support a common framework for the delivery of DMDC applications by creating a five year Indefinite Delivery Indefinite Quantity (IDIQ). These IT services include Enterprise services for DMDC systems and applications as well as Support services for DMDC internal systems and applications that are currently being supported under the Enterprise Information Technology Services (EITS) I IDIQ.

History:
The previous IDIQ contract entitled, "Enterprise Information Technology Services (EITS)" was awarded under H98210-13-D-0003 by the Defense Human Resources Activity (DHRA) Procurement Support Office (PSO). Market research was originally conducted in accordance with policies set for in FAR Part 10.001 by reviewing the following contract vehicles: General Services Administration (GSA)'s IT Schedule 70, GSA's Government Wide Acquisition Contract (GWAC) Alliant, and the Defense Information Systems (DISA) DITCO ENCORE II Information Technology Services.

During Market Research it was determined that awarding this requirement through the AbilityOne program was the appropriate acquisition strategy. As a result, a Sources Sought Notice was issued to AbilityOne Program's Bulletin on October 8, 2012. Global Connections to Employment (GCE) who was currently doing business as Lakeview Center / Gulf Coast Enterprises was selected for award of a five year IDIQ. On March 25, 2013, The AbilityOne Commission sent a letter to DHRA identifying that the EITS requirement has been approved under the Procurement List and that FAR Part 6.302-5, "Authorized or Required by Statute" shall be used as the authority to award a contract to Lakeview Center, Inc.

Current Requirement: As part of market research for EITS II, GSA examined required sources of supply in accordance with FAR Part 8.002. Per this research, DMDC Enterprise IT Services is on the AbilityOne procurement list as required source of supply through the Centralized Nonprofit Agency (CNA) Source America and in turn the designated NPA, Global Connections to Employment (GCE). Since this requirement has successfully been awarded and completed under a contract within the AbilityOne Program, no other market research is required as the Government is required to award the contract to the incumbent AbilityOne contractor.

Per 41 U.S. Code § 8504, Procurement requirements for the Federal Government (a) IN GENERAL.—An entity of the Federal Government intending to procure a product or service on the procurement list referred to in section 8503 of this title shall procure the product or service from a qualified nonprofit agency for the blind or a qualified nonprofit agency for other severely disabled in accordance with regulations of the Committee and at the price the Committee establishes if the product or service is available within the period required by the entity. As such, the Government is required to utilize Source America

Competition: As per FAR 6.302-5(b)(2) (Authorized or Required by Statute), the Government shall use qualified nonprofit agencies for the blind or severely disabled. Additionally, in accordance with 41 CFR

51-5.2(a), "nonprofit agencies designated by the Committee are mandatory sources of supply for all entities of the Government for commodities and services included on the Procurement List." The current contractor has been approved within the AbilityOne Program.

EIT accessibility standards of Section 508: Section 508 applies. This acquisition is for Electronic and Information Technology (EIT). Therefore, Section 508 accessibility standards (http://www.section508.gov/) were incorporated when describing the requiring activity's needs in the PWS.

Commercial Item: The requirement is a commercial item as defined in FAR Part 2.101. A Commercial Item Determination can be found in the contract file.

Fair and Reasonable Determination:
In accordance with FAR 15.404-1(b)(2)(ii)(iv)/(vi), the Government determines GCE's pricing to be fair and reasonable based on comparison with competitive published price lists and comparison of proposed prices obtain through market research for similar items. GCE proposed all labor categories that were provided in RFP attachment 2 "DMDC EITS II Labor Categories and Price Template" and provided discounts. Proposed FFP labor rates for all years have been determined fair and reasonable by favorable comparison to current rates on the GSA GWAC Alliant, Alliant II, as well as the Contract-Awarded Labor Category (CALC) tool using similar labor categories awarded under schedules. Direct labor escalation was determined to be reasonable through a comparison the BLS Employment Cost Index for service providing industries. Therefore overall labor pricing is determined fair and reasonable. A full analysis can be found in the contract file.

Prepared by: MICHAEL LEVY Digitally signed by MICHAEL LEVY Date: 2019.05.13 15:44:03 -04'00'

Michael Levy Date
Contract Specialist, GSA FAS AOD

Approved by: RYAN SCHRANK Digitally signed by RYAN SCHRANK Date: 2019.05.14 07:21:37 -04'00'

Ryan Schrank Date
Contracting Officer, GSA FAS AOD

U.S. General Service Administration

Performance Work Statement (PWS)

For The

Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II
(EITS II)
Indefinite Delivery Indefinite Quantity (IDIQ) Contract

GSA ITSS Order ID No.: ID03180056

Issue Date: 8 February 2019

Revision Date: As listed in Table of Revisions

Table of Revisions

Rev. No.	Rev. Date	Description	Mod No.
1	2/21/19	Updated based on Q&A submission	

Performance Work Statement
DMDC Enterprise Information Technology Services (EITS) II IDIQ Contract

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) in support of the Office of the Under Secretary of Defense for Personnel & Readiness (OUSD P&R), Defense Human Resource Activity (DHRA) requires information technology services to support IT services and systems serving the Federal Government, the Department of Defense (DOD), Service Members and their beneficiaries.

2.0 BACKGROUND

2.1 The Defense Manpower Data Center (DMDC) supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security, and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970s, covering all Uniformed Services, all components of the Total Force (Active Duty, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data for the Uniformed Services. This data supports decision making by the Office of the Undersecretary Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD. DMDC's programs include verifying military entitlements and benefits (e.g., health care, dental, education, and life insurance); managing the DoD Identification (ID) card issuance program; providing identity management for the DoD; employee and Service member travel assistance; personnel and property identification; authentication and access control systems; security clearance, adjudication, and continuous monitoring tools; debt protection for deployed Service members and predatory lending protection for members and their families; personnel evacuation support systems; and assisting military members and their spouses with transition to civilian life. Supporting applications and databases are available to the user community 24 hours per day, seven days per week, with sub-second response time. Any outage can result in disruption of services to DoD beneficiaries as well as potential financial claims from the TRICARE contractors. Additional information about DMDC can be obtained at https://www.dmdc.osd.mil.

2.2 DMDC historically managed programs by lines of business with unique platforms and architectures, limiting the ability to consolidate programs and capabilities to achieve cost savings. In 2017, Under Secretary of Defense for Personnel and Readiness (USD P&R) directed a reorganization of DHRA and DMDC. Under the DMDC Director's direction, DMDC moved to implement a service delivery model with an enterprise-wide architecture to normalize and consolidate legacy applications to enable migration to a virtualized, cloud infrastructure. This transformation of the organization, culture, and programs requires a strategic re-thinking of contracted support and services. To eliminate barriers to standardization, contracts must be aligned to deliver enterprise-wide capabilities vice delivering stand-alone applications and systems.

2.3 The major components of DMDC's IT environment, major programs and software supported by this Performance Work Statement (PWS) are described in Appendices A through L of this PWS. DMDC's portfolio is constantly evolving and growing and as a result, requires development and sustainment support for numerous components, applications, and systems. It is anticipated that during the life of this order DMDC will augment and change tools to improve visualization, usability, speed of delivery of data

and to create a more cost effective footprint. DMDC anticipates that these components, applications and information may change before and during the performance of this contract.

2.4 PROGRAM OVERVIEW & TECHNOLOGY ENVIRONMENT

The major components of DMDC's IT environment, major programs and Commercial-Off-The-Shelf (COTS) products are supported by this PWS. The Contractor shall comply with all applicable laws, policies, procedures, and apply federal Government best practices. The Contractor shall ensure all Cybersecurity and Information Technology projects, applications, systems, programs, or other areas of support provided hereunder comply with, adhere to and are guided by the standard program inception, elaboration, construction, and maintenance application life cycle.

This PWS supports both classified and unclassified programs on multiple external networks and security domains. Services requiring personnel with Secret and Top Secret clearances will be identified in the individual task orders written off of this IDIQ.

3.0 OBJECTIVES

The objective of this contract is to provide IT capabilities and services under an Indefinite-Delivery/Indefinite-Quantity (IDIQ) task order type contract. The Contractor shall have knowledge of business processes, the ability to analyze those processes in a holistic and integrated context, and recommend viable cost-effective technical and data solutions that improve operations and reduce costs. The Government's primary objectives under this contract are to secure an industry partner that:

- Provides flexible, scalable IT services that will enhance each supported activity's ability to respond to dynamic needs in their respective areas of responsibility.
- Delivers operational, technical and program efficiencies to drive down costs without compromising the timeliness or quality of services.
- Optimizes use of tools, technologies, bandwidth, capacity, and computing power in a manner that controls and reduces costs.
- Manages workload surges effectively and in a manner that, given mission requirements and competing priorities, efficiently schedules and applies resources to meet the needs of supported activities without one activity's needs being given primacy over the other.

The effort includes ensuring that systems are fully compatible and integrated with current software programs and functional in relation to existing operating environments to the greatest extent possible.

DMDC's portfolio is constantly evolving. It is anticipated that during the life of this order DMDC will augment and change tools to improve visualization, usability, speed of delivery of data and to create a more cost effective footprint. Lastly, the Contractor shall remain abreast of emerging technologies in the marketplace and recommend changes, modifications, upgrades, and industry best practices.

4.0 SCOPE

The scope of this contract is to provide IT services to support a common framework for the delivery of DMDC applications and systems supported under the EITS II contract. These IT services include the following components:

(a) **Enterprise services for DMDC systems and applications.** These enterprise services will ensure the consistent application of DMDC's service delivery model across DMDC's IT portfolio. Services to be provided under this requirement include enterprise architecture, enterprise application database management, and enterprise quality assurance.

(b) **Sustainment and Enhancement Services.** The scope of the sustainment and enhancement services spans the scope of the systems, applications, and databases that are identified in Appendix A.1 of this PWS.
As DMDC's portfolio changes, the list of systems and applications in Appendix A.1 will evolve during the life of the IDIQ to meet changing mission needs, based on the following:

1) As new programs and requirements are realigned to DMDC's portfolio, the Government will evaluate these capabilities to determine if the capability aligns with sustainment and enhancement requirements already supported within the EITS II portfolio. Requirements that are determined to align with current sustainment and enhancement work is within scope.
2) DMDC programs as they are modernized or realigned within the DoD or another federal agency will be removed from the EITS II portfolio. The Contractor will provide transition out services for these programs. Modernization under the EITS II IDIQ contract means major technical efforts, such as but not limited to:
    - re-platforming
    - re-hosting
    - recoding
    - re-architecting
    - re-engineering
    - interoperability
    - replacement and retirement

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall provide support for the tasks described below:

5.1 TASK 1 – PROVIDE PROGRAM/PROJECT MANAGEMENT SUPPORT

Program Management includes the effective and efficient management of all contractor work including the accountability and security of all personnel. Program Management ensures that contractor performance is within agreed upon quality, cost, and schedule objectives and supports Government planning and decision processes with cost estimates, technical plans, status reports, performance estimates, and other decision support information. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS.

The Integrated Master Plan (IMP) and Integrated Master Schedule (IMS) help establish and maintain that baseline and facilitate effective planning and forecasting that are critical to project success. The IMS includes distinct tasks that are summarized by risk and Work Breakdown Structure (WBS) identifiers so the program can track progress and measure schedule performance. The IMP and IMS should be traceable to the program, contractor WBS and the PWS.

In support of Task 1 - Program and Project Management subtasks, the Contractor shall:

5.1.1 Construct and manage an IMP and IMS including a WBS, critical path milestones, management approach, policies, procedures and suggested project metrics for each task order to provide a high-level picture of all project activities. The Contractor shall update, manage, and analyze proposed schedule changes providing the Program Managers with an assessment of impacts to the IMS in accordance with program, project or initiatives. The Contractor shall submit and maintain the IMP and IMS on the enterprise Microsoft Project server.

5.1.2 Provide information and recommendations to respond to Congressional, DOD, other Government agency, media or industry inquiries, Freedom of Information Act (FOIA) requests, audits and for Congressional testimony.

5.1.3 Maintain a real-time calendar of ongoing projects this includes maintaining, refining, and revising the project collaboration sites currently on SharePoint or other Government-designated repositories. This site must include project overview documents, a consistently updated document library that preserves document history, schedules, a dashboard, assignment and POC lists, summaries and agenda for all meetings and conferences attended, and support for collaborative editing/versioning of project documents.

5.1.4 Provide a Project Management Plan (PMP) that encompasses each awarded task order and that describes the proposed management approach, the milestones, tasks, and subtasks required by the individual task order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities. The Project Manager shall be responsible for a detailed PMP that identifies and assigns tasks, major milestones, dates and dependencies, and indications of critical path. The PMP shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. The Government approved PMP will be used to monitor the Contractor's progress on the task orders. The PMP is an evolutionary document, any revisions are considered incorporated to any subsequent task order, upon written acceptance of the Government, inclusive of any changes to deliverables detailed in the PMP.

5.1.5 Coordinate with DMDC governance bodies such as DMDC Information Systems Security Group (DISSG), Developer's Steering Group (DSG), Enterprise Quality Assurance (QA), Configuration Management (CM), IT Operations, Customer Contact Center (CCC), DMDC Management Advisory Group (DMAG), production support, technical writing, implementation support, and other impacted divisions for project requirements and execution.

5.1.6 Identify, document, and execute risk planning and mitigation strategies that address exposure in the operation, maintenance, delivery, and deployment efforts of DMDC products. Identify and manage technical risk factors, including those related to execution of contract requirements.

5.1.7 Develop, maintain, enhance, and revise all required project documentation including project charters; concepts of operation (CONOPS); business requirements documents; integrated business use cases, user stories, and epics; functional designs and specifications; technical designs and specifications; requirements traceability matrices; process flow and activity diagrams; developer/technical use cases to support DMDC projects and programs; and end-user documentation.

5.1.8 Monitor legislative and policy changes; perform regulatory, legislative, policy and standards research and provide assessments to the government of impact to designated programs and IT products; and implement government directed legislative and policy changes.

5.2 TASK 2 – PROVIDE ENTERPRISE ARCHITECTURE (EA) SUPPORT

Enterprise Architecture is the transformational resource that translates business vision and strategy into effective enterprise change by creating, communicating, and refining the key insights (requirements, principles, models) that describe DMDC's future state and enable evolution and transformation. The goals of the Enterprise Architecture are to improve the organizational efficiency, effectiveness, and

agility by delivering business-aligned future states. Architecture shall comply with DoD and DMDC security policies and models.

5.2.1 Inform and advise DMDC leaders and staff on strategic and operational opportunities for improvement and develop roadmaps that illustrate feasible approaches to achieve them. Provide architectural insight for enterprise and IT-level strategy formation; providing models of future state, with roadmaps that steer the implementation of change initiatives.

5.2.2 Create an EA Vision and Plan that documents current and future state models and includes a roadmap of transitioning from current state to future state. Determine business drivers, constraints, architecture principles, initial architecture requirements, stakeholder concerns and EA deliverables and models to be produced to address these concerns.

5.2.3 Design and implement the architecture for various applications, including hardware, software, mainframe, and data for classified, un-classified, integration among applications, and cross-domain solutions. Identify tools and technologies that meet the new software development requirements as well as the DMDC current architectural approach.

5.2.4 **Business Architecture**

Application Architecture defines the framework of an organization's application solutions against business requirements. It looks globally within systems and designs business processes, selects the best software to support those processes and determines the development of dedicated solutions. It ensures the application landscape is scalable, reliable and complies with DoD and DMDC referenced architectures.

5.2.4.1 Conduct application architecture initiatives; identify and classify application components according to the specific business and performance objectives they support and the technologies employed.

5.2.4.2 Document and perform analyses of the current application inventory and provide detailed application architecture guidelines that improve both business and technology processes and applications.

5.2.4.3 Identify and recommend which applications should be delivered, what technologies should be used to deliver them, and how the applications should be designed, deployed and integrated in the most effective and flexible way. Identify regulations and legislation applicable to each inquiry.

5.2.4.4 Assess and document the alignment of applications and services to Agency programs.

5.2.4.5 Develop and maintain architectural design documents.

5.2.4.6 Identify problems, correctly attribute them to automated processes and/or submission data and develop solutions.

5.2.4.7 Respond to ad hoc research requests from DMDC management to include: performing special studies, conducting data research and respond to inquiries for DMDC internal customers, as well as external customers from within the DoD and the Federal Government.

5.2.5 **Infrastructure & Technology Support**

5.2.5.1 Conduct Enterprise requirements analyses, IT architecture and infrastructure planning, implementation, and maintenance.

5.2.5.2 Provide technology assessment evaluation on hardware and software, document hardware and software technology refresh recommendations.

5.2.5.3 Review and propose changes to charge-back methodologies.

5.2.5.4 Provide support in assessing performance of infrastructure in producing business value and return on investment.

5.2.6 **Enterprise Data Architecture (EDA)**

5.2.6.1 Coordinate enterprise efforts that affect data with a focus on data that moves through the enterprise.

5.2.6.2 Improve the consistency, timeliness, quality, security and delivery of data and streamline data flows eliminating unnecessary costs from the data architecture.

5.2.6.3 Define and document interfaces and movement of data through the enterprise.

5.2.6.4 Ensure data architecture meets performance, maintenance, and system requirements.

5.2.6.5 Create an enterprise-wide set of models, standards, glossaries and hierarchies which allow a standard description of data across business lines, products and functional areas.

5.2.7 **Integrated Solutions Management**
The requirements of this performance area include management and technical support for research, analysis recommendation and documentation of integration issues and approaches. The issues and approaches considered under this area evolve from a variety of sources such as external audits, technical reports, DOD and Federal standards, operational policies and doctrines, technical guidelines and best practices.

The Contractor shall assist the Government in performing the following activities for services required under this performance area:

5.2.8 **Business Process Reengineering (BPR)**
This performance area involves the use of Business Process Reengineering (BPR) as an approach for improving organization performance and covers the range of BPR activities including services needed to implement new or revised business and functional processes arising from BPR undertakings. The Contractor shall assist the government in examining organization goals, objectives, structures/hierarchies, cultures, systems and roles for the purpose of executing a ground-up redesign for achieving long-term, full-scale integration required by the agency. Improving performance and reengineering processes includes services in support of, and helping shape, the direction of DMDC security, including those applications and approaches to network defense required to protect from

unauthorized entry and intrusions, as well as measures designed to track and prevent future damage to DoD's communication capabilities.

5.2.9 **Cloud Implementation, Integration and Operations**
Provide support for integrating new applications and transitioning existing applications into virtualized/cloud environments. This support includes the entire cycle of transition events, from supporting the customer in acquiring cloud service provider enclaves, including market research and piloting efforts, to building out Virtual Data Centers and network architectures, installing applications and locking down environments, transferring any existing databases or other information from existing hosting solutions, supporting assessment and authorization of the new environments, and supporting testing activities in the virtualized environments. This effort also includes integration activities with Platform as a Service and Software as a Service offerings, as well as with other required services or systems (i.e., authentication services). This effort also includes development and implementation of strategies for data and application portability and storage to minimize vendor lock-in and data loss.

5.2.10 **Security Architecture**

5.2.10.1 Verify security systems. Maintain security by monitoring and ensuring compliance to standards, policies, and procedures; conducting incident response analyses; developing and conducting training programs.

5.2.10.2 Develop the architecture that incorporates systems security principles, Information Assurance controls and risk management concepts and best practices into organization-wide strategic planning considerations, core missions and business processes supporting organizational information systems.

5.2.10.3 Enhance security team accomplishments and competence by planning delivery of solutions; answering technical and procedural questions for less experienced team members; teaching improved processes; mentoring team members.

5.2.10.4 Determine security requirements by evaluating business strategies and requirements; researching information security standards; conducting system security and vulnerability analyses and risk assessments; studying architecture/platform; identifying integration issues; preparing cost estimates.

5.3 TASK 3 – PROVIDE ENTERPRISE DATABASE MANAGEMENT (DBM) SUPPORT

5.3.1 Create a Database Maintenance Plan that provides a set of critical specific tasks that need to be performed regularly to ensure adequate database performance and availability.

5.3.2 Define, build, orchestrate and manage database operating procedure run books that support operational processes.

5.3.3 Act as technical consultant to other database administrators; provide direction in planning, design, implementation, operations and management, installation, patching, tuning and configuration of database applications. Define processes and guide efforts for problem resolutions, troubleshoot, make recommendations and take action to ensure optimal performance of databases.

5.3.4 Produce entity relationship and data flow diagrams, database normalization schemas that are logical to physical data maps and data table parameters.

5.3.5 Create stored procedures, functions, views, triggers, constraints and analyze access patterns; proposing the best combination of indexes, constraints, foreign keys, and queries.

5.3.6 Respond to database service requests and contribute to plans and policies for the production management of critical, large and enterprise databases.

5.3.7 Design, implement, maintain, and repair databases for continuous operation. Specific database standards will be defined at the task order level. Generally, databases under this contract shall:

- reduce the time previously required to complete the same task by continuous operations with outages less than 5%.
- be executable in operation at all times unless they are being maintained or repaired.

5.3.8 Instruct application owners on new Relational Database Management System (RDBMS) features; provide analysis, performance impact, ease of use, and compatibility with existing environments.

5.3.9 Define project schema requirements and establish guidance on enterprise modeling standards as they apply to the production and test databases.

5.3.10 Conduct and identify logical database design and modeling, identify physical design requirements, tablespace and partitioning recommendations and collaborate with the data architects and the enterprise data modeler to review and publish application logical data models.

5.3.11 Maintain data integrity and availability for enterprise level databases, tables and structures.

5.3.12 Monitor and tune Structured Query Language (SQL) Data Manipulation Language (DML) statements stored in the database. Write database queries to extract information from the dynamic performance views and database administrator views in the database to identify problems. Collaborate execution of these queries with the systems database administration group and review results.

5.3.13 Monitor project storage consumption, identify storage usage trends and schedule database object reorganization. Coordinate with the application owners to identify project storage requirements and compute storage requirement.

5.3.14 Collaborate with the Configuration Management (CM) Team on deployments and processes.

5.3.15 Provide database restore and recovery in collaboration with IT Operations. Participate in the annual disaster recovery exercises and ‘point in time’ recoveries.

5.3.16 Perform database conversions, migrations and data extracts from production databases.

5.3.17 Support, maintain, and keep the test, development, and pre-production databases and database configurations consistent across environments and conduct database refresh of all database instances.

5.3.18 Verify the accuracy and completeness of the data in DMDC databases (e.g., Personnel Data Repository (PDR), Joint Verification System (JVS), Real-Time Automated Personnel Identification System (RAPIDS)/Common Access Card (CAC)).

5.3.19 Create and maintain a database maintenance dashboard that monitors resources, record application transaction volumes and tracks database volume.

5.3.20 Provide RDBMS network encryption requirements and identify encryption requirements for database connections. Monitor RDBMS log files and application log files for database related problems.

5.3.21 **Control Database Security**

5.3.21.1 Provide a database security plan that identifies all of the assets and data. Document responsible parties, locations, and unique identifiers for these assets providing an auditable record that may be referenced as needed for implementing security measures and investigating incidents.

5.3.21.2 Design data distributions and data archiving solutions with security measures in place to protect against computer threats.

5.3.21.3 Capture and monitor Data Dictionary Language (DDL) actions against test, model office, contractor test/prod sim and production databases. Report any unauthorized DDL activities to the government Information Assurance Officer.

5.3.21.4 Provide guidance to application owners on how to effectively query database tables. Review and suggest query improvements explaining the rationale behind the changes. Advise on RDBMS tools to assist in constructing efficient database queries.

5.3.21.5 Coordinate with developers and end-users on database usage, query development, tuning and to migrate objects and code between different environments.

5.3.21.6 Monitor for deviations—implement appropriate policies and monitor any vulnerabilities that cannot be remediated for any and all activity the deviates from authorized activity.

5.3.21.7 Respond to suspicious behavior—alert and respond to any abnormal or suspicious behavior in real time to minimize risk of attack.

5.4 TASK 4 – PERFORM SOFTWARE DEVELOPMENT LIFECYCLE (SDLC) SERVICES

Provide services for all phases of software design and development including deployment to ensure applications and databases enable users to meet mission goals and objectives **(Appendices D and E)**. These efforts include a wide range of software design, development, implementation and integration, and may include concept development, planning, requirements definition and analysis, systems design and development, coding and testing, production and systems support, deployment, implementation, integration, and software application maintenance.

Software development shall place emphasis on coding that is easily maintained, highly secure and compliant with DMDC coding practices. The Contractor shall maximize and facilitate code re-use by leveraging already existing or project specific software re-use libraries. Executable and source software

generated specifically for this task shall have all rights relinquished to the Government and, at the Government's discretion, be made available for other Government users to obtain.

5.4.1 **Requirements Gathering and Analysis**

5.4.1.1 Perform requirements gathering and analysis to include requirements analysis, feasibility, migration, business process reengineering, requirements validation through interaction with functional proponent, requirements traceability, business process modeling, rules, data requirements, and interface management. Document workflow, business processes, data and services, and include a standard set of artifacts for the purpose of understanding the program asset/software requirements.

5.4.1.2 Translate requirements to design modifications maintaining the integrity of the product's design.

5.4.1.3 Develop user scenarios, user interfaces, and provide oversight of development activities.

5.4.1.4 Provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives.

5.4.1.5 Create data flow diagrams, perform data standardization and perform enterprise modeling, functional economic analysis, simulation/modeling, activity based costing and activity based management support.

5.4.1.6 Provide "as is "and "to-be" functional analysis.

5.4.2 **Design**

Perform design; describe system and software development and implementation processes. Document the requirements to be met by each element of the design and traceability to mission requirements. Document the software architectural design of each element and a description of each software unit.

5.4.2.1 **Software Development**

5.4.2.1.1 Support an agile and interactive development methodology (rapid development) and software development lifecycle with focus on the repetition of abbreviated work cycles and functional requirements. Software development shall be compliant with current DoD , DMDC and CMMI practices, processes and services.

5.4.2.1.2 Perform and document functional and technical requirements, create analysis and design documentation, program specifications, unit test criteria, code and test program units, and produce documentation.

5.4.2.1.3 Document code, conduct code reviews, include technical and functional specifications, applicable DODAF requirements and comply with DMDC configuration management requirements, including consistent application of effective version control. Deliver all software components including source code with release notes.

5.4.2.1.4 Provide Tier Level 3 support (24/7/365) for application outages in production and data issues escalated by the Customer Contact Center (CCC), program manager, or application helpdesk.

5.4.2.1.5 Update applications and infrastructure in support of DMDC infrastructure improvements, changes, technical refreshes, or migrations (e.g., CUF, AION migration, Data Center location transition). Assist the government in converting and testing software to run on new hardware or virtualization platforms.

5.4.2.1.6 Develop and execute Software Test Plan(s) to address application or system use cases, user interfaces, security considerations, and reports using test data designed to demonstrate compliance with all documented functional specifications for each release.

5.4.2.1.7 Perform planning, design, development, test and implementation of various static and dynamic content web sites; maintain and expand existing web pages.

5.4.2.1.8 Submit for review a testing report for each software package to the program manager after each software test; the testing report shall outline the result(s) of the software test plan for each item within the requirements traceability matrix.

5.4.2.2 **Software Maintenance and Sustainment**

Software Maintenance consists of correcting faults, improving performance or other attributes, adapting to a changing organization and technical environment and preventive maintenance. Software Sustainment involves orchestrating the processes, practices, technical resources, information and workforce competencies for systems and software engineering to enable systems to continue mission operations and be enhanced to meet evolving threat and capability needs. Provide all phases of software maintenance as defined in ISO/IEC 14764. The Contractor shall define, develop, trouble-shoot, and resolve problems during maintenance and sustainment. Maintenance shall include, correction, adaptive, perfective and preventive maintenance.

5.4.2.2.1 Create and maintain a Software Maintenance Plan of all maintenance actions. The plan shall indicate which maintenance tasks have been performed, when a particular maintenance task is not performed at its scheduled time and the reason and any future maintenance activities.

5.4.2.2.2 Develop and maintain a Software Quality Assurance Plan that details the subsystem and system level processes used to insure software products are tested and validated. Major events within the Software Quality Assurance Plan shall be reflected in the IMS. Implement a program to provide data quality assurance of software processes and deliverables.

5.4.2.2.3 Document code and version control releases. Deliver source and executable code and supporting documentation.

5.4.2.3 **Unit Testing**

5.4.2.3.1 Developers shall write unit tests to ensure that the unit (be it a method, class, or component) is working as expected and test across a range of valid and invalid inputs. In a continuous integration environment, unit tests shall run every time a change to the source code repository.

5.4.2.3.2 Conduct a verification of the interaction one or more new or modified coded product components, as well as dependent components that have not been modified, to ensure complete coverage of requirements and successful interaction of components prior to full system testing.

5.4.2.3.3 Conduct interface (system-to-system), stress and volume testing, as part of development testing to identify issues as early as possible, reducing the risk and cost of rework.

5.4.2.3.4 Create test data in all testing environments.

5.4.2.3.5 Version and maintain all test artifacts in order to perform repeatable and reliable testing.

5.4.2.3.6 Develop test plans, data and tools that exercise the application at both the unit and systems integration levels.

5.4.2.4 **Release Management**

Support the release cycle of each application to include installation, set-up, testing, and running of applications deployed within four (4) separate DMDC environments (see **Appendix B** for additional information on the environment configurations). Application deployment may require pre-loading of databases with a minimum set of valid test records, and provisioning a minimum number of users in each environment for access to the application(s). Comply with DMDC standards for common builds and apply configuration Management (CM) process specified in the Release Management Charter (see **Appendix E**) to all deployment items. This includes versioning application code for each deployment, building deployment packages, developing (and implementing, if required) back-out plans, recording and reporting the status of the deployed applications, and verifying the completeness and correctness of the deployed applications. Deployments will also require on-site and/or online training to personnel within the DoD community for using the deployed application.

5.4.2.4.1 Definitions for releases are as follows:

a. **Major Release** - Significant new capabilities and features, as well as large-scale defect fixes and occur infrequently. Major releases include significant code re-factoring and new development supporting a combination of major architecture, functional, or user interface level changes within the release.
b. **Minor Release -** Limited set of new features and functionality, tend to be more feature-laden than bug-fix-laden. Minor releases include limited architectural, functional, or user interface level changes within the release. Bug fixes and security patches could also be included.
c. **Maintenance Release** - Addresses defects or enhancements.

5.4.2.4.2 Manage system software, hardware, and configurations, to include patches, emergency data fixes, and upgrades for each release. Inform system users of upcoming releases that will change or increase system functionality or capability.

5.4.2.4.3 Ensure each release is compliant with Risk Management Framework requirements to gain certification as required by DoD Information Assurance and DMDC policies. Ensure monthly IAVA issues are monitored and resolved. Coordinate new releases with stakeholders, hosting facility and owners of connected systems. Coordinate with and allow system access to the Government IA representative for routine testing and data collection as necessary or requested to comply with IA requirements to obtain or retain Authority to Operate.

5.4.2.4.4 **Application Level Change Management**

Manage and maintain the existing automated software build and deployment infrastructure for each deployed application in support of the following environments: stand-alone workstations, LAN/WAN

development, LAN/WAN Test, and LAN/WAN Quality Assurance (QA). This includes but is not limited to overseeing the source code repository, infrastructure, common library components, and scripts required to perform CM automation. Coordinate with DMDC Release Planning to monitor, coordinate and stage required artifacts for each scheduled release. Software will be staged based on scheduled and out of-cycle release planning in support of the following environments. The environments may include the following: stand-alone workstations, LAN/WAN networks, Contractor Test, Stress Test and Production. Government review and approval is required prior to promoting to production environments. Provide a pre-deployment checklist to ensure all software is accounted for in each release and process change requests managed through the DMDC Configuration Management infrastructure.

5.4.2.5 **Configuration Management (CM)**

5.4.2.5.1 Manage the baseline configuration of the platforms, systems, subsystems and apply Configuration Management (CM) techniques that establish and maintain the integrity of the system. Provide configuration control support that includes analysis, change recommendations, tracking and reporting. Identify and document the characteristics of a configuration item, to control changes to a configuration item, and to record and report change processing and implementation status. (See **Appendices G.1 and G.2**).

5.4.2.5.2 Develop and maintain Configuration Management Plan (CMP). The Contractor's methodology must provide CM support for both program and engineering management functions, and apply configuration identification to all program elements whose physical and functional properties need to be managed and directly controlled

5.4.2.5.3 Collect, review, track and archive Configuration Control Documents and deliver all software components with release notes.

5.4.2.5.4 Support functional requirements traceability and the establishment of configuration items and configuration baselines, including functional baselines and product baselines.

5.4.2.6 **Production Support**

5.4.2.6.1 Monitor process and software changes that impact production support, communicate project information to the production support staff and raise production support issues to the product owner. Support scheduled and unscheduled, on-request and end-user initiated processing of business applications.

5.4.2.6.2 Maintain a run log for all batch applications. Implement procedures for proactively identifying, preventing, and responding to problems. Provide ongoing running and monitoring of batch systems, such as the personnel data feeds, Security, Point in Time and Database Extract.

5.4.2.6.3 Maintain and support all Test, Model Office, user acceptance test, benchmark test, stress test, and Production regions, including systems and applications components Support updates and monthly loads of address validation software.

5.4.2.6.4 Develop and maintain Disaster Recovery Activity (DRA) and COOP plans for every required application and interface.

5.4.2.6.5 Provide escalation support to understand, troubleshoot, root cause, log analysis and resolve complex technical issues.

5.4.2.6.6 Provide daily support with resolution of escalated tickets and act as liaison to product and technical leads to ensure issues are resolved in timely manner. Communicate with source of escalation, complete appropriate documentation, and process tickets according to agency methodology.

5.4.2.7 **Requirements Traceability Matrix (RTM)**

Create or update a Requirements Traceability Matrix for all projects. The RTM shall clearly link the new and/or changed requirements to where and how they have been implemented in the system. The RTM shall provide backwards and forward traceability, meaning the RTM documents each requirement from its source through definition, analysis, design, testing, acceptance, and deployment.

5.4.2.8 **Cyber Security/Information Assurance (IA) Support**

5.4.2.8.1 Ensure that all system or application deliverables meet the requirements of DoD and DMDC Information Assurance (IA) policy and that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications. Protect system information and resources according to established security policies and procedures and ensure application code is updated with the latest security patches to minimize security vulnerabilities.

5.4.2.8.2 Provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with DODI 8510.01 Risk Management Framework (RMF). Provide engineering, cyber security and IA services consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02.

5.4.2.8.3 Provide documentation to support RMF Certification and Accreditation processes. Final approval for all IA tasks under this contract belongs to the Information Assurance Officer, Cybersecurity Branch. The Contractor shall obtain final approval from Cybersecurity. All IA-related design decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by the cognizant representative of the Cybersecurity Branch.

5.4.2.8.4 Identify potential program, system, and engineering risks that pertain to cybersecurity; and participate in and support the development of risk mitigation plans and monitoring of risk mitigation activities.

5.4.2.9 **Technical Writing**

Prepare required end user and technical documentation, online help, reference materials, standard operating procedures and release notes. Tasks shall include but not be limited to:

a. maintain configuration management control of all documents
b. develop and maintain documentation related to the hardware, software application, and/or on-line (web site) sources of data;
c. maintain the DMDC documentation library
d. develop and maintain user documentation and on-line help
e. develop training materials and documentation
f. develop documentation of systems, applications, and processes

g. Ensure all documents are properly checked into SharePoint with the proper meta-data and tags allowing easy retrieval of required documents and information

5.4.2.10 **Software and Systems Integration/Implementation**

5.4.2.10.1 Facilitate and monitor the integration, interoperability, and synchronization of enterprise-wide systems and infrastructure solutions and services.

5.4.2.10.2 Develop a systems integration plan to oversee the development of external dependent projects and provide a strategy for the successful integration of all software and hardware into the environment. Plan to include roles and responsibilities, assumptions, internal and external stakeholders, integration/coordination with external organizations, implementation schedules and status, interdependencies of applications, systems integration, design review and acceptance procedures and schedules, user acceptance testing support, privacy and security management (site security, data privacy/security), and defect tracking and resolution.

5.4.2.11 **Software Transition Support**

The Contractor shall provide support for transition of the delivered software/software components to the Government or Government-specified Contractor, to include, but not be limited to, performing software test and verification, training, and corresponding documents that provide information on the use and maintenance of the software and its components. The Contractor shall prepare a project specific Software Transition Plan. The Software Transition Plan shall address products to be turned over (documentation, software, hardware, tools), formats and media, schedules, and support during transition. The Contractor shall include all resources needed to control, copy, and distribute the software and its documentation. The Contractor shall identify at the Test Readiness Review all hardware and software that will be transitioned during each delivery and the time frame of the transition.

5.5 TASK 5 – CONDUCT ENTERPRISE QUALITY ASSURANCE (QA) TESTING

This task ensures that systems, applications and software delivered by the development teams are functional, stable, and secured. Testing personnel shall not be involved in any stage of the software requirements, design or development process. The purpose of the testing is:

a. Verification – Check whether the product meets the stated requirements, specifications or constraints
b. Validation – Determine whether the product achieves its intended purpose and meets the needs of the stakeholder

5.5.1 Conduct enterprise-wide testing to include but not limited to: online and batch processing, thick-client, web applications, web services, operator based and self-service portlets, system to system interfaces, database objects, shared library components, and integration to third party products and external organizations and other related software components.

5.5.2 Define and develop test plans, test scripts, test cases; track and report issues; conduct testing and measure the success during and after testing; and evaluate and document test results. Types of testing includes, but is not limited to:

a. Functional
b. Integration
c. Performance
d. Regression

e. Compliance
f. System/ end-to-end
g. User Acceptance
h. Usability
i. 508 Compliance
j. Stress
k. Load
l. Boundary
m. Exploratory

5.5.3 Produce consistent, cost-effective results that consider security at every phase, identify issues and facilitate speedy implementation of measures to avoid or mitigate risks.

5.5.4 Provide a perspective on tests and results and allow assessment of the technical and operational impact of any identified noncompliance.

5.5.5 Identify, analyze, and document software defects; assist developers in analyzing and resolving defects. Review quality control processes and identify areas needing improvement.

5.5.6 Maintain, test and support QA testing tools.

5.5.7 Conduct Quality Assurance (QA) using documented requirements provided in functional, technical or application release scope specifications.

5.6 TASK 6 - OPERATE THE COMMON ACCESS CARD (CAC) CENTRAL ISSUANCE FACILITY (CIF)

The CIF is the Department of Defense's (DoD) enterprise solution for bulk production and issuance of CAC cards and their PINs for more than 200,000 new recruits and other DoD personnel annually by collecting required demographic and identity information, processing that data to produce the cards centrally, and shipping the cards to pre-determined locations including eight basic training sites, three academy sites, and two officer training schools.

5.7 TASK 7 - SURGE SUPPORT

Surge will be identified in individual task order if required. As an agency of the DoD, DMDC must respond to real-world changes, whether it is a new reform initiative, top-down policies and mandates, or even national security interests and immediate threats. It is essential that DMDC have the IT resources and means to support evolving threats. Projects include, short-term (less than 90 calendar days) response to implement directives, support to cybersecurity-related events, and surge to support complex upgrades. The Contractor shall provide staffing resources within scope of the current contract to fulfill unplanned projects or unanticipated requirements. The Contractor shall use industry best practices and subject matter expertise to execute additional, as–needed, related projects.
Surge support shall include, but is not limited to, the following activities:

a. Additional resources to support the relocation of DMDC applications/systems
b. Rapid capabilities that mitigate or resolve major IT issues, cybersecurity threats, national security events, policy changes, and impacts
c. Implementation of new DoD programs
d. Transition or transfer of existing DoD programs

The Contractor shall account for additional as-needed activities and provide the resources necessary to accommodate them. During the life of this contract the workload in any one area may grow significantly for a period of time. When a surge requirement is identified by the Government, the surge CLIN will be exercised and the surge requirements will be provided to the Contractor in a document specifying the surge requirements, schedule, and expected outcomes. The Contractor shall develop a Surge Plan which shall include, project approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government. Unless specified differently at the task order level, the Contractor shall staff surge resources within 30 calendar days of formal written approval of the Surge Plan.

5.8 TASK 8 – PLANS, REPORTS, AND DOCUMENTATION

5.8.1 Technical Roadmap

Provide a Technical Roadmap that is updated annually which makes recommendations for DMDC consideration to drive innovation, process improvement, efficiencies, and leverages emerging technology. Incorporate lessons learned from the prior year in each annual update. Provide a proposed schedule and milestones for technology recommendations and a recommended approach to reduce Total Cost of Ownership across DMDC's portfolio.

5.8.2 Communications Plan

Develop and deliver a Communications Plan that provides methods, timing, roles, responsibilities and key messages. The Communication Plan shall describe how the Contractor will establish a reliable means of communicating status about the contract to all appropriate stakeholders. It describes what needs and how it will be communicated, who is responsible for communicating with whom and when the communication needs to take place.

5.8.3 Risk Management Plan

The Contractor shall develop a Risk Management Plan that shall address cost, schedule, technical, project, and program risks. The technical risks shall include design, requirement volatility, security, operations, and technology factors. The Contractor shall submit a Risk Management Plan to the COR and shall update the plan at least annually.

5.8.3.1 Document risks in a risk management system and review weekly with Service Delivery Product Owners at a Risk Review Board, with representation from key project areas.

5.8.3.2 Assist in the identification of risks associated with the technologies included in program/project solutions and risks associated with the methods and techniques used to develop those solutions.

5.8.4 Meeting Summaries

The Contractor shall participate in telephone conferences and meetings to discuss on-going technical performance and problems. These calls are used to summarize activities that have been performed since the previous call and discuss the status of activities going forward. The Contractor shall attend additional meetings as specified by the Government and provide meeting summaries. Participate and contribute to various agencies technical meetings to include Technical Working groups and various ad hoc technical tiger teams.

5.8.5 Weekly In-Progress Review (IPR)

Conduct a Weekly In-Progress Review (IPR) to discuss program, project and service status, existing or potential problems, and projected tasks and milestones. The Contractor shall provide updates for activities in the PMP at the IPR. The Contractor shall participate, document, and distribute minutes of regularly scheduled weekly status report meetings. The Contractor shall meet with the Government Program Manager(s) to discuss technical matters, share ideas, review milestones, discuss activities accomplished, discuss new and current issues and work progress, as well as discuss and resolve outstanding administrative or managerial issues.

5.8.6 **Monthly Status Report (MSR) and Senior Management Reviews (SMR)**

The Contractor shall:

5.8.6.1 Deliver, in format approved by the COR, a Monthly Status Report (MSR) slide deck by the 15th of each month. The slides will be presented during Senior Management Reviews to report on the status and progress of the Contractor's previous month's performance of each task order. The final, Government approved, MSR shall be uploaded to the GSA ASSIST portal within two business days following completion.

5.8.6.2 The Contractor shall schedule a Senior Management Review (SMR) briefing no later than 5 calendar days from delivery of the presentation. The SMR will occur by the 20th business day of each month and will include the activities occurring only in the prior month (e.g. presentation on February will cover Jan 1-31).

5.8.6.3 Conduct Senior Management Review meetings each month to brief Government stakeholders on the status of the work being performed under the EITS II contract. In support of each meeting, the Contract shall prepare an agenda and meeting minutes in a clear, concise and orderly manner. Briefing materials shall be made available to all attendees not less than three calendar days prior to time of briefing. The Contractor's Program Manager shall be on site for monthly SMRs, unless forbearance is authorized by the GSA or DMDC COR.

5.8.6.4 The SMR should include data of sufficient detail to monitor the completion of work products against progress as documented in the PWS. Topics to address include but are not limited to:

- Task Order Summary
- Summary of accomplishments for each project
- Deliverables delivered, status of deliverable comments
- Performance Metrics
- Significant Open Issues, Risk, Impact and Mitigation Action
- Summary of Open Problem Notification Reports (PNRs)
- Summary of Open Contractor Discrepancy Reports (CDRs)
- Summary of Issues Closed, in the reporting period, including CDRs and PNRs
- Status of corrective actions
- Integrated Master Schedule
- Milestones achieved or missed
- Burn Rate and funding status by task order
- Number of personnel on contract
- Subcontractor Identification Performance – discuss 1st Tier subcontractors and vendor performance

- Task deliverables timeliness against plan
- Projected Activities for Next Reporting Period
- Upcoming events

The Government reserves the right to modify status reporting requirements at its discretion. The Contractor shall comply with any revised status reporting requirements at no additional cost to the Government.

5.8.7 **Problem Notification Report (PNR)**

The Contractor shall implement and maintain a Problem Notification Reporting system that provides timely notification to government representatives at DMDC and GSA who have responsibility for administering and managing the IDIQ and its task orders.

The Contractor shall provide immediate verbal notification to the DMDC COR when encountering a problem or risk event that significantly impacts the cost, schedule, or performance of the Order (or any deliverable or project under a task order). The Contractor shall provide a written PNR to the DMDC COR and GSA CO/COR not more than three business days after the identification of the problem.

All PNRs must be tracked in the SMR and through in-progress reviews (IPRs) until the Government agrees they are resolved. In the SMR, provide a summary of all open PNRs, as well as PNRs closed during the reporting period.

The PNR shall include, but not be limited to, the nature and sources of the problem and details addressing all data elements identified within the PNR Template provided under **Appendix R**, inclusive of any actual or potential impact on cost, delivery schedule, or deliverables affected; the extent of a delay (if any); steps to be taken to bring performance back on schedule; and corrective action needed to resolve the problems; action required by the Government; and the extent of any anticipated increase on cost (if any) to the Government.

5.8.8 **Contract Discrepancy Report (CDR)**

In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The Contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the Contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

5.8.9 **Semi-Annual Subcontract Reporting**

On a semi-annual basis, the Contractor shall provide Ability-One and Subcontractor reporting data under the contract, segregated for each task order. This data shall include:

- the name of the subcontractor(s),
- the overall percentage of the work (by hours and dollars) supported by the prime and each of the subcontractor(s).
- support provided by Americans with Disabilities (number of FTE and percentage) by task order.

	Name of Prime	Name of Subcontractor 1	Name of Subcontractor 1	Number of full-time Americans with Disabilities Supporting each order	Percentage of work supported by Americans with Disabilities on each order
Task Order 1	% hours by prime	% hours by sub	% hours by sub		
	% dollars by prime	% dollars by sub	% dollars by sub		
Task Order 2	% hours by prime	% hours by sub	% hours by sub		
	% dollars by prime	% dollars by sub	% dollars by sub		
…	…	…	…	…	…
Aggregate Total					

5.8.10 **Transition Plan**

The Contractor shall support any future transitions and integration efforts and provide a plan for transition services to ensure minimum disruption to vital Government business. This plan shall address how the Contractor shall work with the incumbent and Government personnel to ensure that there will be no service degradation during and after the transition-in period (initial ninety (90) calendar day period after date of contract award) and during the transition-out period (ninety (90) calendar day period prior to date of contract expiration). Prior to the end of the period of performance the Contractor shall begin to transition all data, information, training material, all deliverables, etc., to the office (either Government or Contractor) to perform the tasks in the PWS

5.8.11 **Transition-Out Plan**

If programs are transitioning out, the transition-out plan shall be delivered 30 calendar days after GSA notified the contractor of a specific transtion out activity. The Contract shall submit a Contract Transition-Out plan 90 business days prior to end of period of performance of the contract.

5.9 Quality Management System

The Contractor shall establish a quality management system that ensures compliance with applicable federal mandates, terms and conditions of the contract, performance standards, and industry best practices. Consider as part of its Quality Control Plan (QCP) a number of standard approaches toward quality such as the International Standards Organization (ISO) and Systems Engineering Institute/Capability Maturity Model (SEI/CMM) processes. Specific quality requirements may be provided at the individual task order level.

5.9.1 **Quality Control Plan (QCP)**

The Contractor shall maintain a written QCP that shall reflect the Contractor's overall approach, internal management controls and processes for delivery services that meet required performance standards and its procedures for reporting to the Government on identified aspects of quality issues. The QCP shall

identify the means by which the Contractor will ensure quality effectiveness and demonstrate comprehensive management and review of data. The QCP shall describe what is measured, how often it is tracked and provided, who reviews and assures that appropriate action is initiated when trends are unfavorable, who the Government will contact for contractor quality issues, what method and process is used to track and resolve issues, where reports are sent and maintained, and how often quality issues are reviewed and reported. The QCP shall identify how the Contractor identifies and resolves deficiencies, identifies potential improvements, and maintains and makes available to the Government, documentation reflecting quality control inspections and any corrective actions taken. The Contractor shall provide copies of all discrepancies to the COR.

The Contractor's program for Quality Control shall assure that work complies with the requirements of the contract. The QCP will be reviewed for compliance by the Product Owner and COR. The Contractor shall make appropriate corrections and modifications to the plan and obtain acceptance of the plan before the start of the first operational performance period. Updates shall be provided whenever there is a change.

Develop and maintain an inspection system that encompasses all requirements of the task order. The inspection system shall satisfy the requirements within this PWS and shall be designed to keep the Contractor's management informed of all issues affecting quality.

Develop the QCP based on accepted industry standards and detail the processes, procedures, and metrics for assuring quality. The QCP shall also include establishment of capable processes; monitoring and control of critical processes and product variation; establishment of mechanisms for feedback of field performance and implementation of an effective root cause analysis and corrective action system.

5.10 Quality Assurance

The Contractor shall implement Quality Assurance program to increase performance and reduce the risk of projects, operations and associate contractor failure. The program shall emphasize deficiency detection, prevention and address timely corrective actions for unsatisfactory performance.

5.10.1 Prepare a Quality Assurance Plan that describes the Contractor's Quality Assurance Program and submit the original plan and any changes to the COR for approval prior to implementation. The Plan shall describe the Contractor's methods to monitor projects and ensure all PWS requirements are completed in accordance with specifications and industry standards

5.10.2 The Quality Assurance Plan shall include contractor conducted customer surveys. The Contractor shall conduct these surveys to determine customer satisfaction with the infrastructure operations, maintenance services, and provide the results of the surveys to the COR.

5.10.3 The Quality Assurance plan shall include a customer comments and complaint program. The program shall allow identification and correction of validated customer complaints, and provide feedback to the Government and customers on corrective action(s) taken. The term customer refers to customers internal and external to the organizations identified by this individual task orders.

6.0 DELIVERABLES

The Contractor shall submit a draft version of each deliverable and the government will provide written acceptance, comments and/or change requests, if any, in accordance with PWS Section 7.0. The Contractor shall make any corrections and submit the final deliverable, in accordance with the dates listed in the following table and in accordance with PWS Section 7.0:

Note: Individual task orders may have additional deliverables that will be defined within each task order PWS.

PWS Section	Deliverables	Date Due/Frequency
5.1	PMP, inclusive of: • Integrated Master Plan (IMP) Integrated Master Schedule (IMS)	• Draft due within 30 days of contract award • Final due iaw Inspection and Acceptance clause • Updated monthly
5.2.2	Enterprise Architecture Vision and Program Structure Plan	• Draft due within 60 days of contract award and 30 days after each option year is exercised
5.8.1	Technical Roadmap	60 days after contract award and 45 days after each option year is exercised
5.8.2	Communication Plan	10 days after contract award. Updated as needed
5.8.3	Risk Management Plan	30 days after award. Updated as needed.
5.8.4	Meeting Summaries	1 day after the meeting.
5.8.5	Weekly In-Progress Review (IPR)	Written report is due 1 day prior to meeting; the day of the week the meeting will be scheduled will be determined per task order
5.8.6	Monthly Status Report (MSR) and Senior Management Reviews (SMR)	MSR shall be conducted on the 15th working day of each month; electronic copy of brief shall be delivered 3 days prior to the brief.
5.8.7	Problem Notification Report (PNR)	Three days after identification of problem
5.8.8	Contract Discrepancy Report (CDR)	Respond to CDR in accordance with the requests from GSA Contracting Officer
5.8.9	Semi-Annual Subcontract Reporting	The report shall be submitted after each 180 days of performance
5.8.10	Transition Plan	Transition-In Plan-90 Days after Task Order award If programs are transitioning out, the transition-out plan shall be delivered 90 days prior to end of period of performance of the contract.
5.9.1	Quality Control Plan (QCP)	15 days after contract award. Updated as needed

5.10.1	Quality Assurance Plan	15 days after contract award. Updated as needed
8.4	Breach Report	1 calendar day after the breach
8.5	Organizational Conflict of Interest	The contractor shall immediately notify the Government of any potential OCIs and provide mitigation strategies.
8.8	Non-Disclosure Agreement	Prior to any contractor personnel reporting for work on individual task orders
10.1	Post Award Conference	NLT 5 business days after contract award
10.5.1	Tele-work Report	Annually
10.7.2	Trip Reports	5 business days after the trip unless forbearance is granted by the Government
11.2	Staffing Roster	Monthly

7.0 INSPECTION AND ACCEPTANCE

Inspection of all work performance, reports, and other deliverables under this Contract shall be performed by the Technical Points of Contact (TPOCs) designated post award. Acceptance of all work performance, reports, and other deliverables under this Contract shall be performed by the COR designated post award.

Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the government have been corrected. The general quality measures, set forth below, will be applied to each deliverable:

- Accuracy – deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications validity – all deliverables must satisfy the requirements of the government.
- File editing – where directed, all text and diagrammatic files shall be editable by the government.
- Format – deliverables shall follow dmdc guidance. Where none exists, the contractor shall coordinate approval of format with the COR.
- Timeliness – deliverables shall be submitted on or before the due date specified.

7.1 DRAFT DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) business days from Government receipt of the draft deliverable.
Upon receipt of the Government comments, the Contractor shall have ten (10) business days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

7.2 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Government shall provide written notification of acceptance or rejection of all final deliverables within ten (10) business days (unless specified otherwise). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection. If the Government

does not respond within ten (10) business days receipt of a final work product from the Contractor, the product will be considered acceptable by the Government.

7.3 SCOPE OF INSPECTION

Deliverables will be inspected for content, completeness, accuracy and conformance to requirements. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables, as specified in the specific task order(s). The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of deliverables.

The Government requires a period not to exceed ten (10) business days after receipt of final deliverable items for inspection and acceptance or rejection.

7.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the task order(s), the Contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.
For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods
Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.
If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.
All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.
If the Government finds that a draft or final deliverable contains excessive spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Contract and subsequent Task Orders, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the TPOC/COR.

7.5 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten (10) business days of the rejection notice. If the deficiencies cannot be corrected within ten (10) business days, the Contractor will immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within ten (10) business days.

8.0 RECORDS/DATA

The Government will be sole owner of all technical data, software developed, and infrastructure designed under this project. The Contractor shall deliver to DMDC all software, software licenses, data, form, fit and data first produced (including source code), written documents and reports to include, at a minimum, system change plans, various operations procedures and planning documents, meeting minutes, reports, manuals, training text, program management reviews, financial status reports, and any other documents created in support of this agreement or task orders. All system documentation shall be updated to remain current with each software development activity/phase. The Government will

include the actual requirements, formats, delivery schedules and points of contact in each order. DMDC will have unlimited rights as allocated under FAR 52.227-14(b) in all data delivered under the orders. Unless otherwise stated in the orders, the Contractor shall submit deliverables to the COR or his or her designee. The Government will include review times and response to review comments in the orders. The COR will serve as DMDC's focal point for accepting the deliverables unless an order provides for other procedures.

8.1 DATA RIGHTS

The Government requires unlimited rights in any material first produced in the performance of this contract or any task order, in accordance with the FAR clause at 52.217-14. In addition, for any material first produced in the performance of a task order, the materials may be shared with other agencies or contractors during the period of performance of the task order, or after its termination. For any subcontractors or teaming partners, the Contractor shall ensure at proposal submission that the subcontractors and /or teaming partners are willing to provide the data rights required under the task order.

8.2 LIMITED USE OF DATA

Performance of this effort may require the Contractor to access and use data and information proprietary to a Government agency or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others. Contractor and/or Contractor personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to authorize Government personnel or upon written approval of the Contracting Officer (CO). The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner which provides for greater rights to the Contractor.

8.3 DISCLOSURE OF INFORMATION

Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein.

8.4 BREACH RESPONSE

DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, defines a breach as the "actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected." The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, "DoD Privacy Program," May 8, 2007, and DoD 5400.11-R,

"DoD Privacy Program," May 14, 2007. The Contractor shall also comply with federal laws relating to freedom of information and records management. Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated Cyber Security Officer, and Privacy Officer for the contract within one (1) hour. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to DMDC assets, or sensitive information, or an action that breaches DMDC security procedures.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," June 5, 2009; DoD 5400.11-R, and applicable DMDC Privacy Office guidance. The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Information by the Contractor in violation of the requirements of this Clause.
In the event of a data breach or privacy incident involving contractor processes under this contract, the Contractor shall be liable to DMDC for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals.

8.5 ORGANIZATIONAL CONFLICT OF INTEREST

Contractor and subcontractor personnel performing work under this contract may receive, have access to, or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.), or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

8.6 NON-DISCLOSURE REQUIREMENTS

All contractor personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the contract issued which requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, shall execute and submit a Contractor Non-Disclosure Agreement" Form. This is required prior to the commencement of any work on such task order and whenever replacement personnel are proposed under an ongoing task order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the task order. The Contractor shall take the necessary steps in accordance with Government regulations to prevent disclosure of such information to any party outside the Government and to indoctrinate its personnel who have access to sensitive information and the relationship under which the Contractor has possession of or access to the information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information will be used for the profit of any party other than those furnishing the information. The Nondisclosure Agreement for Contractor Employees shall be signed by all indoctrinated personnel and forwarded to the Contracting Officer Representative (COR) for retention, prior to work

commencing. The Contractor shall restrict access to sensitive/ proprietary information to the minimum number of employees necessary for contract/Task order performance.

8.7 CONTRACTOR TRAINING REQUIREMENTS (5 CFR 930.301(1))

If contractors/subcontractors use Government computers, they shall complete DMDC sponsored IT Security Awareness training. Other DMDC mandated training courses include:

- Records Management
- Insider Threat
- Environmental Management System (West cost only)
- Information assurance (IA)/Cyber Awareness Challenge Training
- Privacy act and Personally Identifiable Information (PII) (combined) - Civil Liberties
- Counter Intelligence (CI) Awareness

8.8 SECTION 508 COMPLIANCE

Unless the Government invokes an exemption, all EIT products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

The Contractor must ensure that all EIT products and services proposed that are less than fully compliant, are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any such EIT product or service proposed is not fully compliant with all of the standards, the Contractor shall specify each specific standard that is not met; provide a detailed description as to how the EIT product or service does not comply with the identified standard(s); and shall also indicate the degree of compliance.

8.9 ENTERPRISE-WIDE CONTRACTOR MANPOWER REPORTING APPLICATION (ECMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil. Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013.

9.0 SECURITY REQUIREMENTS

The Government requires the Contractor to establish that applicants working for the Government under this contract are suitable for the job and are eligible for a Common Access Card (CAC) and public trust position at the appropriate level or security clearance prior to the a task order start date.

9.1 SECURITY CLEARANCE REQUIREMENTS

Contractor personnel must be able to obtain and maintain the requiring access to classified information and shall obtain the appropriate security clearance prior to beginning work on this contract or any Task Orders awarded under this contract. DMDC is not responsible for processing Contractor personnel for national security clearance (SECRET). The contractor shall comply with required DMDC personnel security requirements as specified by the Cybersecurity Branch. Interim Clearances will be reviewed upon notification to DMDC Information Security Branch. It is the responsibility of the contractor Facility Security Officer (FSO) to notify DMDC immediately if there is a change in clearance eligibility.

If at any time, any contractor's FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify the DMDC Cybersecurity Branch and remove such person from work under this contract.

Overarching security requirements and Contractor access to classified information shall be as specified in the basic DD Form 254. All contractor personnel with access to unclassified information systems, including e-mail, shall have at a minimum a favorable T1. The contractor personnel shall have the required security clearance prior to arrival to perform the tasks of this contract.

Facility Security Clearance: The work performed under this contract is up to the Top Secret level and shall require Sensitive Compartmented Information (SCI) access eligibility for some personnel. The contractor shall have a final Top Secret Facility Clearance (FCL) from the Defense Security Service (DSS) Facility Clearance Branch (FCB).

Security Clearance and Information Technology (IT) Level: All personnel performing on this contract shall be U.S. citizens. Personnel security requirements will be determined at the task order level.

Investigation Requirements: All personnel requiring SCI, Top Secret or IT-I eligibility under this contract must undergo a favorably adjudicated Single Scope Background Investigation (SSBI) as a minimum investigation. The SSBI will be maintained current within 5-years and re-quests for Special Background Periodic Review (SBPR) will be initiated 90 calendar days prior to the 5-year anniversary date of the previous SSBI or SBPR.

All personnel requiring Secret under this contract must undergo a favorably adjudicated National Agency Check, Local Agency Check and Credit Check (NACLC) as a minimum investigation. The NACLC will be maintained current within 10-years and requests for Secret Periodic

9.2 CAC Requirements

Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this contract:

a) All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).
b) Two forms of identity proofed identification (I-9 document).
c) Be citizens of the United States.
d) Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:
    a. Who do NOT have an active security clearance

b. Will be obtaining a position of trust through DMDC or
c. Have NOT been favorably adjudicated within the last 24 months.

e) Background investigation has been scheduled by OPM.
f) Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

9.2.1 **Position of Trust**

All Contractor personnel with access to DMDC systems or data must comply with DoD Personnel Security Program. All persons on this contract will be designated in a Critical-Sensitive, or Non-Critical Sensitive position (IT-I or IT-II) as determined by the Government per position responsibilities.
Prior to beginning work on this contract, the contractor will complete all required personnel security requirements as specified by the Defense Human Resource Agency (DHRA), Personnel Security Office. Complete and submit a vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust determination.

9.2.2 **Security Clearance Requirements**

All Contractor personnel requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this contract.
DHRA/DMDC is not responsible for processing contractor personnel for national security clearance (Secret, Top Secret, Top Secret/SCI).
The contractor must comply with required DMDC personnel security requirements as specified by the Cybersecurity Division.
Interim Clearances (e.g., Interim-Top Secret, Interim-Secret) will be reviewed by DHRA Personnel Security Office.
It is the responsibility of the contractor Facility Security Officer (FSO) to notify DHRA Personnel Security Office immediately if there is a change in clearance eligibility.
If at any time, any Contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the Contractor shall immediately notify DHRA Personnel Security Office and DMDC Cybersecurity Division and remove such person from work under this contract.

9.2.3 **LAN Access Requirements:**

It is the responsibility of the Contractor to comply with account access requirements as specified by the DMDC Cybersecurity Division.

- Standard User LAN access at a minimum requires:
  a. Completed DMDC personnel security requirements.
  b. Complete DD 2875 Form(s) for all access required.
  c. Submit proof of completion for Personally Identifiable Information (PII) Training.
  d. Submit proof of completion Cyber Awareness Challenge Training.
  e. Adhere to and sign the DMDC Information Systems User Agreement(s).
- Privilege User LAN access at minimum requires:
  a. Completed DMDC personnel security requirements.
  b. Complete DD 2875 Form(s) for all access required.
  c. Submit proof of completion Privilege User Cyber Awareness Challenge Training.
  d. Adhere to and sign the DMDC Privilege Information Systems User Agreement(s).
  e. DoD 8140.01, Cyberspace Workforce Management certification.
  f. Computing Environment (CE) certification(s).

Privilege User must have Computing Environment (CE) certifications for operating system(s) Labor categories to be added		
IAT Level I	**IAT Level II**	**IAT Level III**
Computing Environment (CE)	Network Environment (NE)	Enclave Enviornment (EE)
Help Desk Support	System Adminsitrator	IT Division Chief
Local Administrator	Database Administrator	IT Director
Developer/Programmer	Network Administrator	Domain Administrator
Software Engineer	Application Administrator	Enterprise Administrator
Software Architect	Security Administrator	Backup Administrator
	Mainframe Administrator	
IAM Level I	**IAM Level II**	**IAM Level III**
Privacy Officers	Security Engineer	Cybersecurity Division Chief
Vetting Officer	Security Analysit	Cybersecurity Branch Chief
Disaster Recovery Manager	Security Auditor	Information System Security Officer
Physical Security Officer		Information System Security Manager
IASAE I	**IASAE II**	**IASAE III**
Architect	Architect Branch Chief	Chief Technology Officer
Cross Domain Solution Manager	Security Architect	Architect Division Chief
	Network Architect	Enterprise Architect

Cybersecurity Job Function Mapping to Categories and Level

9.2.4 **Cybersecurity Requirements**

9.2.4.1 The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Instruction 8500.01 Cybersecurity, DoD Instruction 8510.01 Risk Management Framework, NIST SP 800-53 Cybersecurity Controls and Enhancements, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

9.2.4.2 The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDI 8500.01, DoDI 8510.01 and NIST SP 800-53 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

9.2.4.3 Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoD Instruction 8510.01 Risk Management Framework (RMF) and comply with NIST SP 800-53 and annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A) testing in the form of an Authorization to Operate (ATO) and Cybersecurity Risk Assessment. Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of Cybersecurity A&A and FISMA testing

required for any Contractor owned and operated network, facility and/or application processing DoD information.

9.2.4.4 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means. USB Flash drive use is prohibited by DoD.

9.2.4.5 To the extent that the work under this contract requires the Contractor to have access to DoD sensitive information the Contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The Contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

9.2.4.6 The Contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The Contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the Contractor's organization directly concerned with the performance of the contract.

9.2.4.7 The Contractor shall report Cybersecurity incidents to the Cybersecurity Division.

9.2.4.8 The Contractor shall be responsible for safeguarding all government equipment, information and property provided for Contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

9.2.4.9 Contracting work performed shall be done using government provided email and resources. Resources include government furnished equipment. The Contractors company (and personal) computer shall not be used to perform to include store or transmit government work.

9.2.4.10 Final approval for all Cybersecurity tasks under this contract belongs to the Enterprise Service Directorate, Cybersecurity Division. The contractor is expected to obtain this final approval from Cybersecurity. All cybersecurity-related design, decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies, must be coordinated with and approved by the Cybersecurity Division.

9.2.4.11 The Government may terminate this contract for default if Contractor or an employee of the Contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

10.0 CONTRACT ADMINISTRATION

This section provides roles, responsibilities, and contract administration requirements for the EITS II contract and task orders issued under it. Additional contract administration requirements will be designated at the task order level.

10.1 ORIENTATION/POST AWARD CONFERENCE

The Contractor shall participate in a Government-scheduled post-award orientation after IDIQ and task order award or in accordance with Federal Acquisition Regulation Subpart 42.5. Within 5 business days of award the Contractor shall conduct an orientation briefing for the Government. The intent of the briefing is to initiate the communication process between the Government and Contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives. The Orientation Briefing's place, date and time shall be mutually agreed upon by both parties within a week from the date of award. The completion of this briefing will result in the introduction of both Contractor and Government personnel performing work under this contract. The Contractor will demonstrate confirmation of their understanding of the work to be accomplished under this PWS.

10.2 GOVERNMENT POINTS OF CONTACT

GSA Contracting Officer (CO)
Mr. Ryan Schrank
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Ryan.Schrank@gsa.gov
Tel: 215-446-5823

GSA Contracts Specialist (CS)
Michael Levy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Michael.Levy@gsa.gov
Tel: 215-446-5806

GSA Project Manager / Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Scott.Ostrow@gsa.gov
Tel: 215-446-4497

Alternate GSA Project Manager / COR
Ms. Carol Carpenter
E-mail: Carol.Carpenter@gsa.gov
Tel: 301-737-2493

DMDC Points of Contact (POC)
The name(s) and role(s) of DMDC POCs will be designated at time of award.

10.3 CONTRACT TYPE

Tasks orders issued under the EITS II IDIQ contact may be priced on a firm fixed price basis, a labor hour basis, or a hybrid firm fixed price/ labor-hour basis.

10.4 PERIOD OF PERFORMANCE

The period of performance is one (1) 12-month base plus four (4) 12-month option periods.

Option periods will be exercised at the Government's unilateral right in accordance with FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000). The government may extend the term of this contract by written notice to the contractor within thirty (30) calendar days before the contract expires; provided that the government gives the contractor a preliminary written notice of its intent to extend at least sixty (60) calendar days before the contract expires. The preliminary notice does not commit the government to an extension. If the government exercises an option, the extended contract shall be considered to include this option clause. The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months.

10.5 LOCATION OF WORK

DMDC anticipates the majority of work performed under this effort will be by on-site personnel. However, the Contractor shall propose both on-site and off-site for consideration. Places of performance may include: DMDC facilities in both Seaside, CA and Alexandria, VA. Specific places of performance may vary during performance as required to meet government requirements. Other performance locations may be designated at the task order level.

10.5.1 TELECOMMUTING

The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The Contractor must have an established program, subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the Contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task orders shall be approved by the Contracting Officer and the COR prior to commencement. The Contractor shall provide services from their authorized telework worksite location IAW Department of Defense Instructions (DoDI) 1035.01, Telework Policy. The Contractor shall:

- Develop, implement and operate telework programs IAW DoDI 1035.01.
- Delegate authority for telework implementation to subordinate authorities as deemed appropriate.
- Designate a Program Manager to oversee implementation of the telework program.
- Track contractor personnel participation and provide usage data to the COR at the end of each calendar year as an Annual Telework Report.
- Fully train all telework contractor personnel on the telework procedures including information technology and data security, and safety requirements consistent with:
    - the guidance in DoD Directive (DoDD), reference (g) through (j)
    - DoDD 8000.01, Management of the Department of Defense (DoD) Information Enterprise
    - DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)
    - DoDD 8500.01E, Information Assurance (IA)
    - DoDD 5400.111, DoD Privacy Program

The Contractor shall account for and report the teleworkers time spent in the telework status in the same manner as if the employee reported for work at a traditional worksite and track teleworkers time spent in a travel mode away from the alternate worksite during a period that is scheduled for telework.

10.6 HOURS OF OPERATION

The Contractor shall perform the services required under this contract during normal business hours or after hours as may be necessary so that access to the systems may not be interrupted during normal business hours. The window for normal business hours at DMDC is between 8:00 AM and 5:00 PM EST and PST, Monday through Friday, except for Federal holidays (New Year's Day, Martin Luther King Day, Presidents Day, Memorial Day, July 4th, Labor Day, Columbus Day, Veterans Day, Thanksgiving and Christmas).

The Contractor shall be expected at work on all other days and shall provide development services at offsite locations if they are unable to enter closed government facilities.

Other hours of operation may be designated at the task order level.

10.7 TRAVEL

Travel may be required to various locations CONUS, as directed by the Government on a cost-reimbursable basis. The Contractor shall adhere to the following travel regulations (see FAR 31.205-46):
(1) Federal Travel Regulations (FTR) – prescribed by the General Services Administration, for travel in the contiguous United States.
(2) Joint Travel Regulation (JTR) – prescribed by the Defense Travel Management Office
(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

10.7.1 Travel Requests

Before contractor travel is executed, the Contractor shall have travel approved by, and coordinated with the COR. See Appendix O, Travel Request Form.
The Contractor's travel notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Request Form for Government review and approval. The Government shall approve all travel in writing. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and DSSR.
Requests for travel approval shall:

a. Be prepared in a legible manner;
b. Include a description of the travel proposed including a statement as to purpose;
c. Be summarized by traveler;
d. Identify the travel request/travel authorization number associated with the travel;
e. Be submitted in advance of the travel with sufficient time to permit review and approval.
f. Not be considered approved until written approval is received from the COR (email shall suffice in limited circumstances).

The Contractor shall propose and utilize an organized method and format for the tracking and approval process associated with all Travel Requests. The method and format will be reviewed and approved by the COR post award.

10.7.2 **Trip Reports**

The Government will identify the need for a Trip Report (if required) when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel, to include, at a minimum, the name of the employee, location of travel, duration of trip, and POC at travel location.
Trip Reports will be fully documented within five business days of return for Government review. Trip Reports shall be provided for all conferences, IPRs, and travel, unless forbearance is granted by the GSA or DMDC COR.

10.8 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND INFORMATION (GFP/E/I)

GFP will be identified and provided at the individual task order level. The Government will provide all Government Furnished Property (GFP) in accordance with FAR Part 45 guidelines.
Government Furnished Material (GFM) and Government Furnished Equipment (GFE) may be provided to support individual task orders under this IDIQ. Contractors shall be responsible for preventing damage to all GFM/GFE. Contractors shall be responsible for conducting all necessary examinations, inspections, maintenance and tests of all GFE. Contractors shall be responsible for reporting all inspection results, maintenance actions, losses and damage to the Government. If a Contractor loses or damages the equipment, it will be the Contractor's responsibility, in accordance with the contract clauses, to replace or repair the equipment to original or better condition at no additional cost to the Government.

Contractors shall dispose, recycle, or salvage components as directed by the Government. Contractors shall, at a minimum, meet the requirements in accordance with MIL-STD-882E and DoD 5000.02. At the conclusion of each task order PoP, the Contractor shall account for, return, and/or dispose of all GFP within thirty (30) calendar days from completion of the PoP.

10.9 GOVERNMENT FURNISHED INFORMATION (GFI)

The Contractor shall protect Government data and information, by treating the information as sensitive. Sensitive but unclassified information shall only be disclosed to those authorized personnel described in the task order. The Contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards. When no longer required, information shall be returned to Government control, destroyed, or held until otherwise directed by the Ordering CO. GFI will be identified and provided at the individual task order level. The Government will make available to contractors, GFI to include Government forms, publications and documents and access to manuals and materials necessary to perform work under the individual task orders.

The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of information is properly protected. The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under the task order.

Work under specific task orders may require that the Contractor's personnel to have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, section 552a and applicable agency rules and regulations.

10.10 ON-RAMPING

GSA intends to periodically review the EITS II Contract to determine whether it would be in the best interests of the Government to initiate an open season to add new NPAs to the EITS II Basic Contract. The determination is a discretionary unilateral authority of the Government. The total number of NPAs may fluctuate due to various reasons including NPA consolidation, significant changes in the marketplace or advances in technology, general economic conditions, the Government's exercise of the off-ramp process, or other reasons.

10.11 OPEN SEASON PROCEDURES

If GSA determines that it would be in the Government's best interest to open a new solicitation to add new contractors to the EITS II Contract, the GSA Contracting Officer may do so at any time provided that:

a. The open season solicitation is issued under then-applicable federal procurement law;
b. The open season solicitation identifies the total approximate number of new awards that the EITS II Contracting Officer intends to make. The EITS II Contracting Officer may decide to award more or fewer EITS II Contracts than the number anticipated in the solicitation depending upon the overall quality of the offers received;
c. Any NPA that meets the eligibility requirements set forth in the open season solicitation submits a proposal in response to the solicitation;
d. The award decision under any open season solicitation is based upon substantially the same evaluation factors/sub-factors as the original solicitation;
e. The terms and conditions of any resulting awards from a open season solicitation are materially identical to the existing version of the Basic EITS II Contract;
f. The term for any such new awards from an open season solicitation is co-terminus with the existing term for the base EITS II Contract including the option period (if applicable);
g. If awarded a EITS II Contract through the open season authority, any new EITS NPA is eligible to compete for task orders with the same rights and obligations as any other EITS II Contractor; and
h. The award of any new EITS II Contract(s) does not increase the overall ceiling of the Basic Contract.

11.0 CONTRACTOR STAFFING

When hiring and assigning personnel under the contract, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

Specific task orders will identify contractor staff/FTE skillsets that are required at the start of work.

- *The Contactor is responsible for vetting the qualifications of its own applicants and is responsible for ensuring that each individual performing work holds the minimum 8570 baseline and Computing Environment (CE) certification(s) that apply to the functional role that the individual is to perform.*
- *The Contractor is responsible for verifying its own applicants have appropriate suitability determination and ensuring the proper background investigation is conducted based upon the privileged access level and functional role that the individual is to perform.*

11.1 RAMP-UP PERIOD

Work under this contract may require a ramp-up period at the initial state of the period of performance for the Contractor to recruit and hire personnel. If needed, the ramp-up period specifics shall be identified in the Contractor's proposal.

11.2 STAFFING ROSTER

The Contractor shall submit a staffing roster to the COR monthly, no later than the 15th business day of each month, segregated by task order. The staffing roster shall list the names of each employee working on the task order. The roster shall include as a minimum, the Contract Number, Contractor Name, Employee Primary User ID, Employee Last Name, Employee First Name, Current Security Classification, Work Location, Office Number, Phone Number, Primary Project Number, and Secondary Project Number for each employee. The Contractor shall notify the COR of any additions, deletions, or changes within one business day after the change(s).

11.3 CONTRACTOR IDENTIFICATION

All contractor/subcontractor personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression with members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. The Contractor must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Contractor personnel occupying collocated space in a Government facility shall identify their workspace are with their name and company/contractor affiliation.

All contractor/subcontractor personnel that have access to and use of the Government electronic mail (e-mail) shall identify themselves as contractors on all outgoing e-mail messages, including those that are sent in reply or are forwarded to another user. To best comply with this requirement, contractor/subcontractor staff shall set up an e-mail signature ("AutoSignature") or an electronic business card ("V-card") on each contractor employee's computer system and/or Personal Digital Assistant (PDA) that will automatically display "Contractor" in the signature area of all e-mails sent. All work performed shall be conducted using government provided email. Personal or company email shall not be used to perform government work.

11.4 Contractor Training

The Contactor shall provide fully trained and experienced personnel for performance under task orders awarded under EITS II. The Contractor shall train contractor personnel, at its own expense, except under rare circumstances when the CO has given prior approval for specific training to address unique, specialized requirements of the government that are peculiar to a particular task order.

11.5 Labor Categories

The EITS II Basic Contract includes the standard set of labor categories. The Contractor’s standard labor categories and labor rates included in the EITS II Basic Contract’s Pricing Template are hereby incorporated by reference and made a material part of this contract.

11.5.1 Key Personnel

Key personnel are those personnel considered essential to successful Contractor performance.
As a minimum, the Corporate IDIQ Contracts Manager and Corporate Program Manager Key Personnel shall be available at contract start.

The contractor shall designate on-site managers to provide management, administrative, and technical interface with the COR in accomplishing services under this contract. The Contractor shall provide managers that are knowledgeable and experienced in management of all aspects of communications within their designated Area of Responsibility (AOR). These individuals shall be available on a part-time basis during contract transition and full-time by the contract start date.

The Contractor is expected to minimize employee turnover with respect to personnel performing under this Task Order. The Contractor shall not remove or replace any personnel designated as key personnel under this TO without the written concurrence of the CO. Prior to utilizing other than personnel specified in the task order proposal submitted in response to this requirement, the Contractor shall notify the Government CO and the COR. This notification shall be no later than ten (10) calendar days in advance of any proposed substitution and shall include a resume for the proposed substitution and justification in sufficient detail to permit evaluation of the impact of the change on TO performance.

The request shall be written and provide a detailed explanation of the circumstances necessitating the proposed substitution. The Contractor shall submit a resume for the proposed substitute and any other information requested by the COR needed to approve or disapprove the substitution. The COR will evaluate such requests and promptly. The replacement key personnel shall possess skills of equal or greater qualifications to those being replaced. The CO will notify the Contractor of approval or disapproval thereof in writing within five (5) business days of the key personnel substitution notification.

If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the substitution will be denied and the Contractor shall propose an alternate candidate.

If key personnel are proposed for specific task orders, the Contractor shall staff the vacant key position No Later Than (NLT) 14 calendar days after notifying the COR of a key personnel departure. If the position is not filled by the end of the 14th calendar day, the associated hours for this position will be deducted from the invoice. This will apply to both Firm Fixed Price and Labor Hour task orders.

11.5.2 **Corporate Key Positions**

The Contractor shall assign a Corporate IDIQ Program Manager and Corporate IDIQ Contracts Manager to represent the Contractor as primary points of contact to perform Basic Contract level duties, resolve issues and related functions associated with the contract and task orders solicited and awarded under the EITS II IDIQ Contract.

No costs for the Corporate IDIQ Program Manager, the Corporate IDIQ Contracts Manager may be billed to the Basic Contract.

11.5.2.1 **Corporate Contracts Manager**

The Contractor shall provide a Contracts Manager who shall be responsible for the contractual administration of the contract.

11.5.2.2 **Corporate Program Manager**

The Contractor shall provide a Program Manager (PM) who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the Contractor when the PM is absent shall be designated in writing to the KO within 24 hours of contract award. The PM or alternate shall be available between the hours of 07:30 – 16:30 PST.

11.5.2.3 Mandatory Key Personnel Position Descriptions

The following Contractor personnel are essential for successful accomplishment of the work to be performed under the resultant contract and are defined as Key Personnel. The Government anticipates needing Key Personnel at the task order Level depending on the complexity of the requirements. The Government may require that these positions to be staffed in a full-time capacity for the duration of each order concurrently for multiple Task Orders.

All costs associated with the Contractor Key Personnel positions listed below shall be handled in accordance with the contractor's standard accounting practices:

11.5.2.3.1 Quality Assurance (QA) Manager
Candidate must be knowledgeable of SDLC methodologies and industry best practices such as the IEEE Standard 1012-2004 for Software Verification and Validation and SEI CMMI level 3 procedures and processes.

11.5.2.3.2 Senior Enterprise Architect (EA)
Candidate shall have a bachelor's degree in information technology or related field (e.g., Federated Enterprise Architecture Certification), and relevant senior level work experience with enterprise architecture and CompTIA Security+.

11.5.2.3.3 Senior Database Engineer
Candidate shall have a bachelor's degree in information technology or related field Database architecture and design experience in planning and implementing large-sized database and cloud database technology.

11.5.2.3.4 Senior Software Engineer (SSE)
Candidate shall have a bachelor's degree in information technology or related field. Candidate shall have advanced technical expertise and shall have performed as a technical lead responsible for the development of solutions. The SSE shall have the ability to manage the entire software development lifecycle.

11.5.2.3.5 Senior Information Security Analyst
Candidate shall have a bachelor's degree in information technology or related field. Candidate shall have significant experience with DoD's RMF, DIACAP, NIST Certification & Accreditation and possess a DoD Security+ or CISSP Certification.

11.5.3 **Unique Professional Skills**
Unique professional skills are defined as those bona fide executive and highly specialized skills for which the expertise required or duties performed are within the EITS II Contract's scope, but are so specialized or rare that they are not explicitly defined in any of the EITS II standard labor category descriptions. If a unique need arises, the NPA may propose a specialized labor category outside of the labor categories established in the EITS II Contract. The contractor shall submit an explanation justifying the need for this specialized skillset. The contractor shall comply with all the applicable contract clauses and labor laws, including the Service Contact Act or the Davis Bacon Act, as applicable.

The GSA Contracting Officer will determine whether circumstances warrant use of unique professional skills. Based on price or cost analysis, the GSA Contracting Officer will negotiate a fair and reasonable labor rate with the Contractor at the task order level.

11.5.4 **Technical Refreshment**

After contract award, the Government may implement technical refreshment of the scope and/or the labor categories consistent with FAR 52.212-4 in order to improve performance or react to changes in technology.

11.6 Subcontracting

The Contractor shall not enter into subcontract agreements without approval of the Contracting Officer and the Contracting Officer representative. The Contractor will be notified within five (5) business days by the Contracting Offficer whether the subcontractors has been approved or not approved. All subcontracts shall include the identity of the subcontractor, the extent of the work, the reason for subcontracting.

11.6.1 **Subcontracting Considerations**

There are two related considerations that take center stage. The first is the Limitations on Subcontracting, and the second is what is known as Pass Throughs. EITS II prime NPA(s) are responsible for managing the workload mix being performed under their contract(s) and Orders.

In accordance with the 13 CFR 125.6, and associated FAR Clause 52.219- 14, a small business concern contracting for services will perform at least 50 percent of cost of the contract incurred for personnel with its own employees. Similarly, EITS NPA(s) are expected to perform a meaningful amount of work/add significant readily-identifiable value on each Order to prevent pass-through situations. This is an area of increasing regulation, as evidenced by the DoD interim rule for pass throughs cited in GAO report GAO-08-269, January 25, 2008, and as identified in Section 866 of the Duncan Hunter National Defense Authorization Act of 2009, P.L. 110-417 ("DHNDAA" or "NDAA 2009").

It is a best practice for GSA Contracting Officers to require industry partners to disclose the amount of work they intend to perform with their own resources in Order RFQs and RFPs. The GSA Contracting Officer may require Order invoice level subcontracting reporting should they wish to monitor these matters closely during Order performance. A good rule of thumb at the Order level is for the NPA to be expected to perform approximately 80% or more of the work itself, or to follow specific customer agency standards (such as those promulgated in DoD's interim rule cited above).

It is reasonable and routine that on larger tasks small business prime contractors may manage capacity building through subcontracting with other small business firms and other than small business firms to provide scalability in the early stages of performance. It is reasonable to consider the total prospective life cycle of an order, including option periods, when evaluating how much work the prime plans to perform for a given task order. The GSA CO may request a well-defined plan from NPA prime contractors to facilitate this review, and may qualitatively evaluate such plans during task order evaluation if required under the task order solicitation.

Consent to subcontract pursuant to FAR 44.2 is applicable on an ad hoc basis at the Order level. The GSA Contracting Officer may require subcontractor responsibility determinations of prospective subcontractors per FAR 9.103 and 9.104-1. Consent to subcontract is not required at the Basic Contract level.

11.7 Cooperation With Other On-Site Contractors

When the Government undertakes or awards other orders or contracts for additional work the Contractor will: (1) fully cooperate with the other Contractors and Government employees, and (2)

carefully fit its own work to such other additional contracted work as may be directed by the COR. The Contractor shall not commit or permit any act that will interfere with the performance of work awarded to another Contractor or with the performance of other Government employees. In any case where, in the course of fulfilling the order requirements, the Contractor disturbs any work guaranteed under another separate contract, the Contractor shall restore such disturbed work to a condition satisfactory to the COR and guarantee such restored work to the same extent as it was guaranteed under the other contract.

12.0 APPENDICES

Appendix A.1 - EITS II Portfolio
Appendix A.2 - Overview of DMDC Major Programs
Appendix B - DMDC IT environment Overview
Appendix C - DMDC Computing Environments
Appendix D - SDLC - Process Handbook
Appendix E - Release Manager Charter
Appendix F - Enterprise DBA Standard Operating Procedure (SOP)
Appendix G.1 - Configuration Management Policy
Appendix G.1 - Configuration Management Handbook
Appendix H - Development Steering Group Charter
Appendix I - Quality Assurance Testing Guidelines
Appendix J - Incident Management Service Restoration Team (SRT) Standard Operating Procedure (SOP)
Appendix K - DMDC Information Assurance Policy
Appendix L - Cyber Security Common Language
Appendix M - DD 254
Appendix N - DMDC Senior Management Review Format
Appendix O - Travel Request Form
Appendix P - Quality Assurance Surveillance Plan
Appendix Q - Performance Requirements Summary
Appendix R - Problem Notification Report (PNR) Template
Appendix S - Contract Discrepancy Report (CDR) Template
Appendix T - CPARS Form and Ratings Definitions
Appendix U - EITS II Labor Categories & Labor Category Descriptions *(included in Price Template)*

Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services (EITS) II
Contract # -

Enterprise Architecture
EITS II Task Order 03
Order ID: 47QFMA18K0030-0006

1.0 Introduction

The Defense Manpower Data Center (DMDC) requires baseline enterprise wide information technology services that can support its full range of Information Technology (IT) services in order to develop, sustain and deliver new products, develop and maintain new IT systems, and design, deploy, and maintain the underlying infrastructure. The support will align IT resource expenditures with business goals and objectives and will enable an IT environment with innovative solutions that are responsive to organizational requirements.

2.0 Background

DMDC operates major programs that include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD pay and benefit systems; personnel and property identification, authentication, and access control systems; personnel evacuation support systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and post-service job searches.

The DMDC Enterprise Architecture (EA) provides overarching architecture data and content to drive enterprise capability thread development and traceability. The DMDC EA is developed as a tightly coupled operational extension of the overarching Business Enterprise Architecture. Detailed architecture development efforts provide content to support expansion of both the DMDC Architecture EA and the Integrated Business Framework Data Alignment Portal (IBF-DAP) in specific business focus areas. The detailed architecture provides the information needed to support policy initiatives, investment management and portfolio analysis, and architecture federation with the Services and Components. The DMDC Architecture effort also supports development of architecture for enterprise and/or Component initiatives.

The major components of DMDC's IT environment, test environments, major programs and Commercial off the Shelf (COTS) and Government off the shelf (GOTS) software supported by this PWS are described in the Appendices.

3.0 Scope

DMDC's portfolio of services includes 58 functional programs with 141 supporting systems varying in size and scope and is consistently evolving. This effort provides the personnel, and management necessary to support the strategic management of that portfolio as well as the design and implementation of the supporting architectures for the corresponding customer facing, internally shared, and supporting services. These architectures include business,

application, data, and infrastructure models used to create an integrated, enterprise views that accelerate the transformation of business and technical systems as required to meet strategic goals by providing useful and timely information and removing obstacles to current and future transformations.

4.0 Requirements. The contractor shall:

4.1 Provide Enterprise Architecture Sustainment Support

4.1.1 Support the Government Architecture Program Management, working with leadership and subject matter experts, to build DMDC's EA. The EA provides holistic view of the organization's strategy, processes, information, and information technology assets.

4.1.2 Support the development and sustainment of policies, standards and guidelines for the structure, data, and models in the EA repository. The EA repository model structure includes the following layers: 1) business architecture 2) application architecture, 3) data architecture, 4) infrastructure architecture, and the Technical Reference Model that shall integrate security requirements throughout these layers.

4.1.3 Work with all DMDC internal and external stakeholders to complete business and IT architecture planning.

4.1.4 Assess DMDC business drivers and IT capability and perform gap analysis.

4.1.5 Support the development and sustainment of the IT vision and business/IT alignment statements.

4.1.6 Support the establishment and documentation of the alignment of IT, business, and functional goals and objectives.

4.1.7 Support DMDC's strategic analysis of business and technology, to include assessment of requirements and long-term courses of action.

4.1.8 Support the development and sustainment of strategic roadmaps to meet DMDC business, application, data, and infrastructure goals in the EA repository.

4.1.9 Ensure that strategic roadmaps are supported by underlying models and data in the EA repository.

4.1.10 Research new Enterprise Architecture techniques and standards from the government and industry to implement best practices, refine knowledge, and provide guidance through assisting or providing formal and informal knowledge transfer to DMDC staff.

4.1.11 Support Enterprise Architecture maturation efforts by assisting in the identification, recommendation, and documentation for process improvements, new process adoption efforts, and tool adoption. Identification and documentation of issues and recommended resolution support such as, process mapping, point papers, process research, reengineering, and implementation support, micro-services, legacy data sources, and enterprise architecture frameworks to support the alignment of enterprise's business and IT capabilities.

4.1.12 Support the research of, and provide recommendations for the current and future use of cloud computing environments to include private, public, and hybrid cloud computing environments.

4.1.12.1 Support development of enterprise architecture standards for artifacts, viewpoints, and models to support business decision-making capabilities. Develop and sustain the following enterprise-level Department of Defense Architectural Framework (DoDAF) artifacts: All Viewpoints (AV-1, AV-2), Operational Viewpoint (OV-1), Capability Viewpoints (CV-1 through -4), Project Viewpoints (PV-1 through -3) and Data and Information Viewpoint (DIV-1). Support development of program and product-level DoDAF artifacts.

4.1.12.2 Respond to ad hoc research requests from DMDC management to include; performing special studies, conducting data research and respond to inquiries for DMDC customers.

4.2 **Provide Business Architecture Sustainment Support.**

4.2.1 Provide business architecture support that provides information for decision making for the Government regarding effective IT investments that support business requirements. The business requirements supported by the contracts are linked to the DMDC and Division level Strategic Plans, and provide maximum business value to customers, both internal and external. The business architecture must comply with the guidelines established in the DoD Enterprise Architecture and Business Enterprise Architecture (BEA).

4.2.2 Support the evaluation of business capabilities, gap analysis of business architecture components, and documenting recommended solutions.

4.2.3 Support the development and sustainment of business architecture models within the EA repository such as program architectures, requirements models, service models, and capability models.

4.2.4 Support the development and sustainment of Business Architecture documentation and DoDAF artifacts such as All Viewpoints (AV-1, AV-2), Operational Viewpoint (OV-1), Capability Viewpoints (CV-1, -2 and -4), Project Viewpoints (PV-2 and -3) and Data and Information Viewpoint (DIV-2).

4.3 **Provide Data Architecture Sustainment Support.**

4.3.1 Assist in defining, prioritizing, and requirements gathering for assessing the As-Is data management solution and provide recommendations for effective decision-making capabilities.

4.3.2 Support the development of the Data Governance/Stewardship Framework within DMDC for data ownership for associating file service content with projects, departments, organizational and/or business units.

4.3.3 Support the development and maintenance of comprehensive Data Architecture models in the EA repository.

4.3.4 Assist in defining, recommending, and maintaining Structured Query Language (SQL) and non-Structured Query Language (NOSQL) databases standards, models, processes, and roadmaps.

4.3.5 Work with all DMDC internal and external stakeholders in order to develop data architecture planning and implementation initiatives.

4.3.6 Provide analysis, recommendations, and assistance associated with the Database Architecture Maintenance for both SQL and NOSQL databases.

4.3.7 Support the development of processes to validate and verify consistency and compliance to DMDC architectural standards, processes and report findings and recommendations.

4.3.8 Support logical database design and modeling. Collaborate with the data architects and the enterprise data modeler team to review and publish application logical data models.

4.3.9 Support the evaluation of database structures based on information provided by application owners for DMDC data modeling naming standards, entities, relationships, attributes, and data structure compliance.

4.3.10 Document data reference architectures in DMDC's Technical Reference Model (TRM) in the EA repository.

4.3.11 Support Data Architecture documentation and corresponding DoDAF viewpoints and models artifacts to support conceptual data modeling logical and physical views for current and future business systems, and data exchange interfaces.

4.4 **Provide Application Architecture Sustainment Support.**

4.4.1 Support the documentation and maintenance of current-state application inventory, deployment details, and DoDAF viewpoints and models artifacts. Documentation maintenance must occur in the EA repository. The documentation must include full system and asset inventory and provide reporting capabilities at the request of the Government.

4.4.2 Support application architecture initiatives, such as, identifying and classifying application components according to the specific business and performance objectives they support and the technologies they employ.

4.4.3 Support documentation and analyses of the current application inventory and provide detailed application architecture guidelines to improve both business and technology processes and applications in the interest of integration and cost containment.

4.4.4 Document infrastructure reference architectures in DMDC's Technical Reference Model (TRM) in the EA repository.

4.4.5 Support analysis of core application activities and application components.

4.4.6 Assess and document the alignment of applications/services to programs.

4.4.7 Work with key stakeholders to support application architecture planning, implementation, and maintenance.

4.4.8 Support the development and recommendation of performance metrics for assessing performance of applications and provide a report for return on investments analysis and evaluation of information business systems.

4.4.9 Support development of Application Architecture documentation and create DoDAF artifacts to support business requests, such as audits requests. Artifacts deliverable, such as All Viewpoints (AV-1, AV-2), Operational Viewpoint (OV-1), Capability Viewpoints (CV-1, -2 and -4), Project Viewpoints (PV-2 and -3) and Data and Information Viewpoint (DIV-2) would need to be created for compliance reporting activities.

4.5 **Provide IT Infrastructure & Technology Sustainment Support.**

4.5.1 Support the development and sustainment of the technology standards.

4.5.2 Support the development and sustainment of the technology portfolio.

4.5.3 Support the development and sustainment of the as-is and to-be technology architectures.

4.5.4 Support the development of analyses reports, such as 1) Impact Analysis, 2) Gap Analysis, and 3) Performance Metrics.

4.5.5 Support the coordination of requirements gathering with internal and external stakeholders to resolve conflict for Architecture standards, business processes, and policies.

4.5.6 Support the maintenance of the current state infrastructure inventory at the Enterprise baseline configurations level, deployment details, and information to enable configuration management. Provide reporting capabilities.

4.5.7 Support the documentation of enterprise infrastructure requirements gathering and analysis that supports function and capability traceability matrices between infrastructure and applications.

4.5.8 Support DMDC and Divisional groups in IT architecture/infrastructure planning, implementation, and maintenance.

4.5.9 Support technology assessment evaluations.

4.5.10 Support the development of modernization recommendations as requested based on industry best practices, to design, develop, and implement architecture to meet strategic goals.

4.5.11 Support the identification of, and roadmaps for, the common capabilities required by DMDC services.

4.5.12 Support the maintenance of the Deployable Technology List (DTL) within the TRM.

4.5.13 Provide support for analysis and management of big data and high-fidelity data (data that preserves the identity, context, detail and relationships of business topics)

4.5.14 Support the gap analysis, documentation, and recommendation of methodologies to consolidate infrastructure to reduce variety, version. Technology rationalization is the review and reduction, virtualization, or redistribution of technology, software, or infrastructure to ensure maximum operational capability and flexibility for the lowest cost.

4.5.15 Document infrastructure reference architectures in DMDC's Technical Reference Model (TRM) in the EA repository.

4.6 **Provide DMDC Enterprise Architecture Repository Support**

4.6.1 Conduct administration for the DMDC EA repository, currently implemented in the COTS Sparx Enterprise Architect (Sparx EA) product, to include system installation, troubleshooting, product patching and upgrades. The contractor must be able to gain privileged access to provide administrative support of the EA platform.

4.6.2 Provide training, application support, project design consulting, and documentation based on migration activities, product updates, and other software administration changes.

4.6.3 Provide a monthly report of the DMDC toolset floating license utilization including volume usage as an input to the annual product licensing analysis.

4.6.4 Develop, document, and implement the Standard Operating Procedure (SOP) for the maintenance of the Sparx EA Toolset, to include backup and restore procedures.

4.6.5 Process daily user support requests to manage views, activities, and access control.

4.6.6 Monitor user activities on a daily basis and make process improvement recommendations the Enterprise Architecture Repository as problems areas are discovered.

4.6.7 Respond to daily user requests for assistance related to minor recovery tasks such as reinstituting deleted versions, resolving failed deliveries, failed rebases and baseline tasks

4.6.8 Support DMDC software development project teams with the creation of new projects, streams, and merges when necessary in accordance to new Enterprise Architecture Processes.

4.6.9 Archive and/or remove outdated projects, streams, activities with application team’s approval on a quarterly basis.

4.6.10 Identify, develop, document, and support implementation of process to address promotion of changes of various repository levels through production. Develop a schedule of activities for Government approval.

4.6.11 Validate and reinforce modeling standards and guidelines through a quarterly audit of existing projects. Provide report to Government lead on a quarterly basis to determine actions to be taken.

4.6.12 Prepare and present formal and informal presentations and training content to various levels of the organization and provide formal and informal training to end-users. Formal training shall be scheduled based on the approved Government schedule. Informal training shall occur on an as-needed basis based on interactions with end-users.

4.6.13 Develop and document standard and ad hoc reports and other processes to automate repository functionality as needed.

4.7 Provide Architectural Engagement Support.

The Architecture Division engagement support has varying support requirements. Individuals assigned to engagement tasks may be embedded within project teams for an extended period of time while in other situations they may be available to provide assistance to development teams on an as-needed basis for short durations, for example to assist with specific technical or design issues. In all cases, engagement activities are intended to assist the Architecture Division in the promotion of DMDC's EA System Development Lifecycle.

4.7.1 Assist the government in clarifying the requirements, deliverables, and milestones of the MOU for the engagements.

4.7.2 Providing senior level Java Enterprise Edition (JEE) development and architectural expertise for the project engagements.

4.7.3 Supporting alignment with DMDC standards and processes (e.g. Enterprise Architecture and Capital Planning and Investment Control (CPIC)).

4.7.4 Support and maintain the EA team's collaborative environment to build trust and confidence both within the team itself and associated stakeholders.

4.7.5 Supporting compliance with DMDC Software Development Lifecycle (SDLC) processes and standards by mentoring project teams and providing feedback to the government for process improvements.

4.8 Provide Enterprise Security Architecture Sustainment Support

4.8.1 Support the development of standards for EA repository models to address security requirements.

4.8.2 Support the assessment of EA repository models to ensure systems security principals, Information Assurance controls, and risk management concepts and best practices are incorporated.

4.8.3 Provide monthly security compliance reports to demonstrate that all models in Sparx meet security standards.

4.8.4 Provide security support for organization-wide strategic planning considerations, core missions and business processes.

4.9 Provide Enterprise Architecture Governance Support

4.9.1 Provide administrative support for the management of the architecture governance. Architecture Governance is currently chartered at the Architecture Review Board (ARB). This support includes any future refinements to governance processes to include creation of working groups or other architecture governance related procedures.

4.9.1.1 Coordinate meeting logistics including rooms, communications, and schedules.

4.9.1.2 Ensure required information is provided before topics are added to the schedule to include conducting pre-brief meetings as required.

4.9.1.3 Maintain meetings minutes and action items coming out of architecture governance meetings.

4.9.2 Provide administrative support for DTL management. The DTL process, a sub function of the ARB, provides information that is recorded in the DTL component of the TRM.

4.9.2.1 Maintain notes and action items for technology requests as part of the ARB DTL review process

4.9.2.2 Document final results of the ARB technology review in the DTL.

4.9.3 Support and maintain the Enterprise Architecture Change Management Process ensuring all architecture artifacts are covered by the process. Report on gaps, recommend solutions, and develop and implement approved solutions.

4.9.3.1 As dictated by the Change Management Process, review change requests for EA impact. Where required, ensure that appropriate architecture governance procedures are initiated to maintain the accuracy and completeness of the models in the EA repository.

4.10 Enterprise Architecture Development Support (OPTIONAL TASK)

The Contractor Shall:

4.10.1 Enterprise Architecture Support

4.10.1.1 Develop artifacts in support of the development and sustainment of policies, standards and guidelines for the structure, data, and models in the EA repository. The EA repository model structure includes the following layers: 1) business architecture 2) application architecture, 3) data architecture, 4) infrastructure architecture, and the Technical Reference Model that shall integrate security requirements throughout these layers.

4.10.1.2 Develop artifacts in support of the development and sustainment of strategic roadmaps to meet DMDC business, application, data, and infrastructure goals in the EA repository.

4.10.2 Business Enterprise Architecture Support

4.10.2.1 Develop artifacts in support of the development and sustainment of business architecture models within the EA repository such as program architectures, requirements models, service models, and capability models.

4.10.2.2 Develop artifacts providing business architecture support that provides information for decision making for the Government regarding effective IT investments that support business requirements. The business requirements supported by the contracts are linked to the DMDC and Division level Strategic Plans, and provide maximum business value to customers, both internal and external. The business architecture must comply with the guidelines established in the DoD Enterprise Architecture and BEA.

4.10.3 Data Enterprise Architecture Support

4.10.3.1 Develop artifacts in support of the development of the Data Governance/Stewardship Framework within DMDC for data ownership for associating file service content with projects, departments, organizational and/or business units.

4.10.3.2 Develop artifacts in support of the development and maintenance of comprehensive Data Architecture models in the EA repository.

4.10.4 **Application Enterprise Architecture Support**

4.10.4.1 Develop artifacts in support of the documentation and maintenance of current-state application inventory, deployment details, and DoDAF viewpoints and models artifacts. Documentation maintenance must occur in the EA repository. The documentation must include full system and asset inventory and provide reporting capabilities at the request of the Government.

4.10.5 **Infrastructure Enterprise Architecture Support**

4.10.5.1 Develop artifacts in support of the development and sustainment of the technology standards.

4.10.5.2 Develop artifacts in support of the development and sustainment of the technology portfolio.

4.10.5.3 Develop artifacts in support of the development and sustainment of the as-is and to-be technology architectures.

4.10.5.4 Develop artifacts in support of the development of analyses reports, such as 1) Impact Analysis, 2) Gap Analysis, and 3) Performance Metrics.

4.10.5.5 Develop artifacts in support of the documentation of enterprise infrastructure requirements gathering and analysis that supports function and capability traceability matrices between infrastructure and applications.

4.10.5.6 Develop artifacts in support of the identification of, and roadmaps for, the common capabilities required by DMDC services.

4.11 **Enterprise Data Modeling Support (OPTIONAL TASK)**

4.11.1 Determine project schema requirements and establish guidance on enterprise modeling standards as they apply to the production and test databases.

4.11.2 Participate in logical database design and modeling. Collaborate with the data architects and the enterprise data modeler team to review and publish application logical data models.

4.11.3 Evaluate and recommend database structures based on information provided by application owners (e.g. application upgrades or releases).

4.11.4 Analyze the database maintenance dashboard or reports, which monitor resources, record application transaction volumes and track database volume and make recommendations to improve performance.

4.12 **REPORTS AND MEETINGS**

4.12.1 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

Prior to the delivery of the monthly SMR, the contractor shall also hold monthly pre-SMR meetings with designated Government representatives for each awarded task order. The purpose of the pre-SMR meeting shall be to present the same documentation that will be presented at the

official SMR while also reviewing each task order's specific task order data (listed above). Each contractor task order manager shall coordinate the pre-meeting, distribute the pre-meeting materials and facilitate any changes to the task order's data through the DMDC COR and contractor Program Manager.

4.12.2 **Problem Notification Reports**
The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

4.12.3 **Participate in a Kick off meeting.**
This meeting shall provide an introduction between the Contractor personnel and Government personnel who will be involved with the contract. The meeting shall provide the opportunity to discuss technical, management and security issues. The Kick off meeting will aid both the Government and Contractor in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable. The Contractor shall provide a written summary of the Kick off Meeting.

4.12.4 **Quality Control Plan (QCP)**
The Contractor shall follow the requirements identified in PWS Section 5.9.1 of the EITS II Base IDIQ

4.12.5 **Risk Management Plan (RMP)**
The Contractor shall follow the requirements identified in PWS Section 5.8.3 of the EITS II Base IDIQ.

5.0 Deliverables

All deliverables and work products shall be submitted to the COR in electronic format for acceptance and approval. The acceptance of deliverables and satisfactory work performance shall be based on the timeliness, accuracy and standards as specified in the requirements of the PWS.

Deliverable	PWS Reference	Delivery Date
DoDAF Viewpoints	4.1.13	10 days after each request
Data Reference Architectures	4.3.10	90 days after award
Application Reference Architectures	4.4.4	90 days after award
Infrastructure Reference Architectures	4.5.15	180 days after award
EA Repository product upgrade	4.6.1	180 days after award
Sparx Maintenance SOP	4.6.4	90 days after award
Monthly Sparx modeling Standards compliance report	4.6.11	15th of each month
Sparx Security Compliance Reports	4.8.3	15th of each month
ARB Meetings minutes	4.9.1.3	Within 24 hours of each ARB meeting
Senior Management Review (SMR)	4.12.1	15th of each month with read ahead materials to the COR 3 days prior to SMR.

Problem Notification Report	4.12.2	3 days after identification of problem.
Kick Off Meeting Minutes	4.12.3	Within 3 days of Kick Off Meeting.
Quality Control Plan	4.12.4	Updated upon request by Government.
Risk Management Plan	4.12.5	Updated upon request by Government.
EA Repository Standards	4.10.1.1	(Optional) 30 days after CLIN start
Strategic Roadmaps	4.10.1.2	(Optional) 90 days after CLIN start
Business Architecture Programs	4.10.2.1	(Optional) 120 days after CLIN start
Business Architecture External Service Models	4.10.2.2	(Optional) 60 days after CLIN start
Business Architecture Internal Service Models	4.10.2.2	(Optional) IAW DMDC's Service Catalog Management (SCM) BPR schedule
Business Architecture Capability Model	4.10.2.2	(Optional) 90 days after CLIN start
Data Stewardship Framework	4.10.3.1	(Optional) 90 days after CLIN start
Data Architecture Models	4.10.3.2	(Optional) 60 days after CLIN start
Application Architecture Models	4.10.4.1	(Optional) 60 days after CLIN start
Technology Standard Catalog	4.10.5.1	(Optional) 30 days after CLIN start
Technology Portfolio Catalog	4.10.5.2	(Optional) 30 days after CLIN start
As-is and To-be Technology Architecture	4.10.5.3	(Optional) 120 days after CLIN start
Analyses Reports	4.10.5.4	(Optional) within 15 days of request
Infrastructure Requirements Matrices	4.10.5.5	(Optional) 90 days after CLIN start
Capability Modernization Roadmaps	4.10.5.6	(Optional) 60 days after CLIN start
Government Furnished Equipment (GFE) Inventory List	7.0	30 days after award

6.0 QUALITY SURVEILLANCE

The Government may follow the Appendix P - Quality Assurance Surveillance Plan) to EITS II IDIQ Base Contract

6.1 The table below identifies the Critical Performance Elements and the respective Performance Standards and Acceptable Quality Levels (AQLs) which the Government will use to determine contractor performance.

6.2 Performance Objective and Thresholds:

Architecture Specific Performance Objectives	Architecture Specific Performance Threshold	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection

Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection

6.3 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
  Timeliness – Deliverables shall be submitted on or before the due date specified

7.0 **Contract Administration.**

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

7.1 Contract Type: The contract type for this Task Order will be firm fixed price

7.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award with two one-year options.

7.3 PLACE OF PERFORMANCE / HOURS OF OPERATION: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and

approved by the Government. Occasional travel may also be required, as noted in PWS Section - Travel.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET (8 a.m. to 5 p.m. PT for contractors located on the West Coast), Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

7.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

7.5 Points of Contact:
DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. Dave Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contract Specialist (CS)
Mr. Raj Singh
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: rajdeep.singh@gsa.gov
Tel: 215-446-2868

GSA Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Scott.ostrow@gsa.gov
Tel: 215-446-4497

7.6 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Sections 10.8 thru 10.9 of the EITS II Base IDIQ

7.7 Travel: The cost reimbursable not-to-exceed travel limit is estimated at $5,000.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR. All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

7.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

In addition, certain contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances, as directed by the Government. Contractor personnel shall possess these security clearances at Task Order award.

8.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

9.0 APPENDICES

Appendix A – DMDC ARB Charter Enclosure 1 References
Appendix B – DMDC ARB Charter Enclosure 2 Required Artifacts
Appendix C – DMDC ARB Charter Enclosure 3 Process Map and Description
Appendix D – DMDC ARB Charter
Appendix E - Change Management - Process Handbook v1.0

Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
DMDC Enterprise Initatives

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) requires enterprise wide information technology services that can support the full range of IT services in order to develop, sustain and deliver new products, develop and maintain new IT systems, and design, deploy, and maintain the underlying infrastructure. The support will align IT resource expenditures with business goals and objectives and will enable an IT environment with innovative solutions that are responsive to organizational requirements.

2.0 BACKGROUND

DMDC has integrated new functionality in the Share point tool in the past year. In this PWS, these requirements are being driven by the need to sustain functionality of the enterprise Sharepoint tool. The tools that were developed or enhanced over the past year include eAdmin, eAgreements, eCorrespondence, and INEED.

3.0 SCOPE

The Contractor shall provide all necessary personnel and management required to support business tool automation sustainment.

4.0 REQUIREMENTS:

4.1 Provide Development and Sustainment Support for the automation of Business Tools

4.1.1 Sustain the DMDC and DHRA support tools in the Defense Information Systems Agency DOD Enterprise Portal Service(DISA DEPS) environment in order to effectively implement DHRA and DMDC streamlined processes.

4.1.2 Support the implementation of new processes in accordance with the DMDC business process reengineering initiatives. Develop and implement tools to automate or streamline new, DMDC approved business processes.

4.1.3 Ensure changes are recorded in a configuration management database and released software and documentation is archived in a software library in accordance with DMDC policy.

4.1.4 Prepare and execute milestone reviews for requirements, design, development and testing as required by the DMDC organization issuing the task order, to ensure the development meets the needs of the Government.

4.1.5 Provide industry best practices, practical assistance, and a high level of technical support, during and after implementation to ensure implementation is seamless and successful.

4.1.6 Coordinate testing and initial fielding of new software releases of business tools. Develop and monitor implementation schedule.

4.1.7 Distribute release notes and communication impact to customers for software releases to user acceptance, benchmark, stress test, and production regions.

4.1.8 Develop and maintain user manuals to support DMDC business tools in accordance with industry standards. The user manuals shall provide detailed instructions on how to use the DMDC business tools, where to obtain additional information, to ensure quick resolution of user issues and reduce help desk calls.

4.1.9 Develop quick reference guides for frequently executed workflows within DMDC business tools.

4.1.10 Provide user support for business tools to ensure timely resolution of user issues.

4.1.11 Provide transition support for business tools transitioning from DISA DEPS to other platforms (e.g. Task Management Tool (TMT), ServiceNow). Transition support includes providing functional and technical requirements details for DISA DEPS and supporting data transfer from DISA DEPS to other platforms.

4.2 KICK OFF MEETING

4.2.1 Participate in a Government scheduled Kick-off meeting within 5 calendar days of Task Order award. The purpose of this Kick-off meeting is to aid both the Government and Contractor personnel in achieving a clear and mutual understanding of all task requirements, and achievable deliverables within funding constraints; and identify and resolve potential problems. The Contractor shall be prepared to discuss any issues requiring clarification and gather information as necessary to support each deliverable. The contractor shall submit meeting minutes the DMDC PM and GSA COR NLT five (5) days after meeting completion.

4.3 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.4 Expenditure and Resource Report (ERR)

Provide an Expenditure and Resource Report (ERR) to the Government COR on a monthly basis. This report shall detail by PWS Task, each project that is being worked by the contractor, the amount that will be billed to the Government and the resources assigned to that task. Each report shall report on the previous month and provide the current month and cumulative task order costs by project.

4.5 QUALITY SURVEILLANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

4.6 Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the DMDC PM or GSA COR or GSA CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

4.7 Problem Notification Reports (PNR).

The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ.

5.0 Performance Standards

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection

Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection
Meet all Government and agency specific requirements	100% compliance	100% inspection to ensure that all Government and Agency specific requirements have been met. Independent verification of security procedures-defined by agency (could be performed by a third party or another agency according to current security regulations and measures).
Project Plan	100% of areas required by government including the WBS are created and updated monthly. On time delivery of Initial and Monthly Updates	100% Inspection

5.1 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, shall be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

5.2 The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the task order. The Contractor's QCP (PWS 4.4.1) shall be incorporated into and become part of this task order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the task order and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the contract.

5.3 The Contractor shall maintain a Lessons Learned document, updating it subsequent to each software release, disseminate and make recommendations to the Government to increase the quality of future deliverables and improve reliability and efficiency of systems. The Government will use a Quality Assurance Surveillance Plan (QASP) as part of the Government's efforts to monitor contractor performance.

6.0 DELIVERABLES

6.1 The Government will provide written acceptance, comments and/or change requests, if any, within 10 work days from Government receipt of the draft deliverable using the Deliverable Acceptance Checklist.

Deliverable	PWS Ref.	Due Date
Project Plan	4.1.1	30 days after award
Release notes	4.1.7	NLT production release
Business Tools User Manuals	4.1.8	NLT production release; updates within 10 business days of Government request
Business Tools Quick Reference Guides	4.1.9	NLT production release; updates within 10 business days of Government request
User Support Requests	4.1.10	Provide an initial response to all user support requests within 1 business day

7.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

7.1 Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets, copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

7.2 The Government will provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; commercial off-the-shelf software; hosting facilities;

and all other relevant materials and equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support.

8.0 PLACE OF PERFORMANCE / HOURS OF OPERATION

8.1 The work under this task shall be performed on site at DMDC facilities in Seaside, CA. Any work performed at other locations must be identified in the formal submission and approved by the Government.

8.2 The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

8.3 The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following:

- Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.
- Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment

9.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order will be 12 months from date of award.

10.0 TRAVEL

10.1 The Government does not anticipate travel. The following applies if travel is necessary.

10.2 Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. All travel shall be coordinated in writing

through the DMDC Client Representative and travel must be pre-approved by the GSA CO (or their designated representative) prior to incurring costs.

10.3 All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

10.4 Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

10.5 Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

11.1 The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

11.2 In addition, all contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. In addition, personnel with access to CE production data must have a fully-adjudicated Single Scope Background Investigation (SSBI) and Security+ certification at time of award.

11.3 The Government requires the contractor to establish that applicants or incumbents either employed by the Government or working for the Government under this contract are suitable for the job and are eligible for a public trust position at the appropriate level at the start of the PoP date. This includes the following:

- US Citizen
- Favorable FBI fingerprint check
- Fully adjudicated background investigation completed

11.4 SECURITY CLEARANCE REQUIREMENTS

Contractor personnel must be able to obtain and maintain the requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this contract.

11.4.1 DMDC is not responsible for processing contractor personnel for national security clearance (SECRET).

11.4.2 The contractor must comply with required DMDC personnel security requirements as specified by the Information Assurance Branch.

11.4.3 Interim Clearances will be reviewed upon notification to DMDC Information Security Branch.

11.4.4 It is the responsibility of the contractor FSO to notify DMDC immediately if there is a change in clearance eligibility.

11.4.5 If at any time, any Contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the contractor shall immediately notify the DMDC Information Assurance Branch and remove such person from work under this contract.

11.5 CAC REQUIREMENTS

11.5.1 Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this contract:

11.5.2 All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).

11.5.3 Provide two forms of identity proofed identification (I-9 document).

11.5.4 Be citizens of the United States.

11.5.5 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:

- Who do NOT have an active security clearance
- Will be obtaining a position of trust through DMDC or
- Have NOT been favorably adjudicated within the last 24 months.

11.5.6 Schedule a Background investigation by OPM.

11.5.7 Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

11.5.8 Obtaining CAC or PIV ready status is the responsibility of the contractor. It is the responsibility of the contractor to notify DMDC when this is complete.

11.6 POSITION OF TRUST REQUIREMENTS

11.6.1 All contractor personnel with access to DMDC systems or data must comply with DODI 5200.2-R and DODI 8500.2. All persons on this contract will be designated as either an IT-I or IT-II as determined by the Government per position responsibilities.

11.6.2 Prior to beginning work on this contract, the contractor will complete all required DMDC personnel security requirements as specified by the Information Assurance Branch.

11.6.3 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust.

11.6.4 It is the responsibility on the contractor to ensure their employees and sub-contractors (if applicable) comply with DMDC personnel security requirements.

11.7 LAN Access Requirements:

11.7.1 It is the responsibility of the contractor to comply with account access requirements as specified by the DMDC Information Assurance Branch. At minimum:

- Completed DMDC personnel security requirements.
- Complete DD 2875 Form(s) for all access required.
- Submit proof of completion for Personally Identifiable Information (PII) Training.
- Submit proof of completion Information Assurance/Cyber Awareness Challenge Training.
- Adhere to and sign the DMDC Information Systems User Agreement(s).

11.7.2 Information Assurance Requirements:

The contractor and all contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Information Assurance (IA), DoD Instruction 8500.2 Information Assurance (IA) Implementation, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

11.7.3 The contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDD 8500.1 and DoDI 8500.2 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

11.7.4 Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoDI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to DIACAP must present evidence of Certification and Accreditation (C&A) testing in the form System Identification Profile (SIP), DIACAP Implementation Plan (DIP), DIACAP Scorecard and Plan of Action and Milestones (POA&M). Evidence of FISMA compliance must be presented in the form of a POA&M. The contractor will be responsible for the cost of IA C&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

11.7.5 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

To the extent that the work under this contract requires the contractor to have access to DoD sensitive information the contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

11.7.6 The contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the contractor's organization directly concerned with the performance of the contract.

11.7.7 Contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the Contracting Officer Representative (COR) and corrective actions will be implemented immediately.

11.7.8 The Contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

Government may terminate this contract for default if Contractor or an employee of the contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

11.7.9 The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

12.0 INSPECTION, ACCEPTANCE AND PAYMENT

12.1 The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services. The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

12.2 Delivery Address. All deliverables shall be submitted to the designated DMDC POC's. Additionally, if directed, the Contractor shall upload the deliverables into the GSA ITSS Portal.

12.3 Method of Delivery. The Contractor shall provide all deliverables and reports in the format of which to be defined or approved by the Government and subject to change over the course of the task order.

12.4 Acceptance Criteria. Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in EITS Contract H98210-13-D-0003 and all terms and conditions of this Task Order, including all modifications.

12.5 Acceptance of Deliverables. The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 days, the Contractor shall not assume that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 working days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

12.6 INVOICING

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

Table of PWS Revisions

Rev. No.	1.1.1 Rev. Date	Name	1.1.2 Description	TO Mod No.
1	8/12/19	SO	Added Sections 5.13 (Provide Quality Assurance Support for ACTUR Applications) and 5.14 (Provide Quality Assurance for Accountable Car Organizations (ACO) Demonstration).	2

Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Enterprise Quality Assurance Support
Order ID: 47QFMA18K0030-0005/ID03180056001

1.0 Introduction

DMDC requires Quality Assurance (QA) testing for enterprise wide support for several applications within the DMDC portfolio. The major components of DMDC's IT environment, test environments, major programs, Commercial off the Shelf (COTS) and Government off the shelf (GOTS) software supported by this PWS are described in the attached Appendices.

2.0 Background

DMDC operates major programs that include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD pay and benefit systems; personnel and property identification, authentication, and access control systems; personnel evacuation support systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and post-service job searches.

With the higher adoption of continuous integration and the constraint of reduced budgets within the Department of Defense, DMDC's goal is to operate with automated and efficient processes to realize increased quality productivity with a decreased budget. With this task order, Quality Assurance shall adhere to the DevOps methodology. DevOps allows for continuous releases and deployments with continuous testing and monitoring which aims at building, testing and releasing software faster, smarter, and more secure. Successful Quality Assurance (QA) in the DevOps environment depends on automated application testing, collaboration with development team and business owners, and improving processes. This requires a cultural shift of the current enterprise QA environment to work on prevention versus detection.

During this task order, DMDC plans to implement a DevOps environment that allows for continuous integration. The Quality Assurance team will have access to all QA tools and will remain responsible for application automation tools (Redwood and Selenium).

Historical workload for 2017 to 2018 may be located in Appendix N and for a sample of descriptive overviews for applications currently supported by QA, refer to Appendix C (this list is not all-inclusive of the applications that may be supported by Enterprise QA).

3.0 Scope

3.1. The contractor shall provide the personnel and management necessary to provide test data management and Quality Assurance testing for DMDC's software components, to include: online and batch processing, web applications, web services, operator based and self-service portlets, system to system interfaces, database objects, shared library components, and integration to third party products and external organizations and other related software components. Applications provide releases to address requirements changes, security improvements, technology advances, bug fixes, etc. DMDC maintains approximately 200 applications.

3.2. The Government requires a total of 500 releases to contractor test or production environment during this period of performance of 12-months from date of award, during which that the Contractor shall support and provide Quality Assurance testing. A re-release to production due to leaked defects shall not be counted as an additional release. Leakages that are preventable by QA include: bugs that are testable in the pre-prod environment; application does not work as intended per release notes. The Contractor shall notify the GSA Contracting Officer, the GSA COR, and the DMDC COR, in writing when the releases to production reach 75% of the period of performance baseline. The Contractor shall also notify the Government when it has reasons to believe that the annual amount of releases to production will surpass the baseline amount. Within this notice, the Contractor shall propose a cost estimate for successful support of the additional releases beyond 500. The Government anticipates that the implementation of DevOps will enable faster, more frequent releases. However, the Contractor should leverage the automated application testing included in the scope of this effort to release software faster and more efficiently.

4.0 Objective

The objective of this task order is to provide quality assurance testing that ensures requirements meet the needs of the customer and test data management while maximizing efficiencies through automation. The

objective is for the development and maintenance processes are continuously improved to produce products that meet specifications.

5.0 Requirements. The contractor shall:

5.1. Planning and Management of Quality Assurance

5.1.1. Provide an updated Quality Management Plan (QMP) within 15 days of award that defines how Quality Assurance (QA), Quality Control (QC), and Risk Assessment will be conducted. When developing the QMP, the QA Contractor shall review and use as key input the following: all available planning artifacts including any guidance provided by DMDC in writing or orally; and International Organization for Standardization (ISO) 12207. The QA Contractor shall adhere to generally accepted industry practices, such as Agile, for project quality management and software development quality assurance management. At a minimum, the QMP shall include the following:

- Staff roles and responsibilities
- QA Workload Statistics
- Detailed plan for QA Review, including scope, criteria, and methodology to be employed
- Project Schedules
- Risk Assessment Methodology
- Quality checks

5.1.2. Provide a project plan that outlines the management approach, milestones, tasks and subtasks required to attain 50% automation (as outlined in 5.3; 5.3.15) for the application suites as represented by the applications in section 3.2 release count by the close of the task order. The project plan shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates to meet this requirement. Outline the strategy and parameters used to determine the order of applications automated with the objective of maximizing efficiencies and incorporate this strategy into the current QA Test Strategy outlined in 5.1.3. The project plan shall be completed within 15 days of task order award, and finalized with government approval within 30 days of task order award.

5.1.3. Maintain and update QA Test Strategy that outlines the contractor process used to: validate that all tested items perform as designed, fulfill requirements, meets any applicable service level agreements (as outlined per project) and does not adversely impact other applications. Outline the major activities, techniques, and tools that will be used.

5.1.3.1. Incorporate the Contractor strategy for automation implementation and the QA transition to DevOps as part of the QA Test Strategy. The QA automated testing shall exist, run, and operated within the DevSecOps infrastructure.

5.1.3.2. Incorporate the Quality Assurance Test Strategy consistent with existing DMDC QA standards, guidelines, and documented templates as outlined in the appendices.

5.1.3.3. Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage. Current BPR tools include Sparx Enterprise Architect, Microsoft Project Server, and Change Gear but could change throughout the life of this order. ServiceNow is in the implementation process and is expected to be in use at DMDC during this task order. Once implemented, ServiceNow shall be used to manage testing efforts.

5.1.3.4. Adhere to the configuration management process.

5.1.4. Measure the success during and after quality assurance testing. Success shall be measured through metrics which detail to the Government the: percentage of test case execution, test case pass rate, trend defect analysis, defects by severity, and defect leakage rate. Metrics shall be provided monthly with SMR documentation and made available on the QA SharePoint site post testing and upon request. Please refer to section 7.3 for a definition of the metric terms.

5.1.5. Analyze the defects that were leaked into production, or to user acceptance, and provide a summary report monthly with SMR documentation; at a minimum, include:

- Determination where the defect was leaked (e.g., CT or Production)
- Cause for leakage (e.g., test case was not created, requirement missed, requirement not defined, etc)
- Remediation (what the contractor will do to rectify the current leak, such as building appropriate test case, etc)
- Mitigation for future (what the contractor will do to assure this will not occur in the future)

5.1.6. Maintain all QA related artifacts on a Government provided SharePoint site.

5.1.7. Provide a Staffing Plan (SP) no later than (NLT) 10 calendar days after Task Order (TO) award. A copy of the comprehensive written SP shall be submitted to the GSA Contracting Officer, the GSA COR, and the DMDC COR within 5 working days when changes are made thereafter. Contractor's SP shall detail the contractor's approach to test support across DMDC's application portfolio. This approach shall include the contractor's methodology to:

- Continue to provide timely and high quality support when key contractor personnel are out of office or responding to other urgent QA requirements;

- Provide staffing redundancy to mitigate any deterioration to the timeliness or quality of performance in cases of staff turnover or surge in QA requirements
- Provide staffing redundancy to maintain automation framework development and sustainment
- Maintain a staff that can support automated testing

5.1.8. Maintain the standard for QA automated best practices for development teams to leverage during the software development lifecycle. The best practices shall outline automation dependencies, rationale for consistent naming standards by development teams, and other items required from development teams to support a robust automation testing framework.

5.1.9. Maintain the catalog that defines the level of QA efforts required for each type of projects conducted, based on type of application, number of elements within the scope of the project, deployment environments, shared components, interaction with COTS products, etc. The catalog shall be readily available on the DMDC SharePoint site and available upon request.

5.1.10. Participate in meetings within functional, technical, operational, and strategic areas to contribute to various agency level discussions including but not limited to analysis and design, enterprise QA initiatives, working groups and various ad hoc tiger teams. This includes participating in functional requirement meetings and/or recurring project meetings to incorporate new features/ enhancements to an application for the purpose of understanding the requirement and scope of the QA role and to better define the level of QA effort for a given task or project.

5.1.11 Quality Control Plan (QCP)
The contractor's Quality Control Plan (QCP) shall be submitted no later than (NLT) 10 calendar days after task order award. A copy of the comprehensive written QCP shall be submitted to the Contracting Officer (CO) and Contracting Officer's Representative (COR) within 5 working days when changes are made thereafter. After acceptance of the quality control plan the contractor shall receive the Contracting Officer's acceptance in writing of any proposed change to his QC system.

5.1.12 Risk Management Plan (RMP)
The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this task order. The Contractor shall create, modify, maintain, and implement a task order-wide Risk Management Plan. The accepted Risk Management Plan shall be incorporated into the Order and submitted no later than (NLT) 10 calendar days after task order award.

5.2. Quality Assurance Testing

Provide support primarily within the DMDC identified QA regions for next generation development and production simulation, with the provision for QA support within other regions, including external hosted sites as required (the regions QA primarily works in are detailed in Appendix D). Requests for QA support outside of the QA regions will be reviewed by the applicable government leads for the QA and requesting division(s) for action as needed. Next generation development includes code being developed that shall replace what is in production. Production Simulation is code base currently in production.

The applications that are tested on the Enterprise Quality Assurance task order come from several different software development contracts within DMDC; it is imperative that communications remain open amongst other contractors. The tasks for completion within QA testing include:

5.2.1 Analyze and review requirements from the product team at the inception phase to assure clear and testable requirements and/ or user stories are provided. Provide feedback to the product team. QA shall be involved in code coverage analysis prior to Sprint closure, recommending that the appropriate levels of Junit test cases have been implemented.

5.2.2 Create and/or maintain a test plan for each project that requires Quality Assurance and review with project team(s) to ensure full coverage of test cases. The QA Test Plan is provides a detailed listing of all QA activities within each QA testing project; a sample template may be found in Appendix E. QA Test Plans shall be developed and maintained for all projects requiring QA level support. At a minimum, test plans shall outline:

- Sign off approval required
- Level of effort
- Resource estimate
- Schedule
- Planned tests cases
- Test cases traced to requirements
- Test method(s) necessary
- Entrance and exit criteria
- Assumptions
- Risks

The test case matrix and RTM locations should be identified in the test plan, for traceability purposes.

Provide the underlying information that is required within each QA test plan as outlined in the following sections:

5.2.3 Collaborate with project teams and develop test cases that are based on all requirements/ user stories. Test cases shall be created based on realistic scenarios that may occur in the production environment and shall cover 100% of outlined requirements.

5.2.4 Provide clear mapping between the user stories or requirements of tested software and the underlying test case(s) supporting complete coverage and validation of the provided functional requirements.

5.2.4.1 Update Requirements Traceability Matrix (RTM) for all projects that require quality assurance. Collaborate with the underlying project teams to review the functional requirements and/ or user stories in support of mapping these requirements to existing QA test cases, and identifying new QA test cases required to support the requirements. Assure the test cases provide accurate and realistic test case coverage for the functional area(s). Test cases shall provide coverage for all requirements. Update test cases as necessary and keep test cases current and meaningful throughout the life of the project. An overview of the RTM, including roles and responsibilities is outlined in Appendix G.

5.2.5 Defined method of testing (e.g., regression, exploratory, smoke, etc.), as agreed upon with the government point of contact. QA test plans shall accommodate regression testing of software components and functionality that has not been modified but may interact with modified components and functionality to ensure that changes have not adversely affected existing capabilities.

5.2.5.1 Collaborate with the underlying project teams to review the test plan and receive government approval.

5.2.6 Conduct testing and validate software is ready for the production and/or user acceptance environment by utilizing the appropriate test method agreed upon in the test plan.

5.2.7 Ensure, at a minimum, the following criteria shall be met before concluding testing (some or all of these functions may be automated):

- No open blocker or critical priority issues
- All items outlined in the scope according to the test plan behave as expected
- All issues resolved as “fixed” are verified
- Tests defined in test plan run and behave as well as or better than current production version of application
- 100% of test cases identified were executed and verified
- Full regression test completed (exceptions require approval by the Government technical point of contact and project lead)

5.2.7.1 Ensure all automated and manual QA Test Case Suites include the QA test transactions and corresponding results processed and ensure the reports are maintained and available for the government. The results of the executed test cases (pass/fail/reason for failure)

5.2.8 Follow and support the practices and configuration management processes per DMDC guidelines.

5.2.9 Log and track issues, defects, enhancements, etc., found during testing via the DMDC provided issue tracking and reporting system within 2 business days of discovery. Report and communicate Issues found to the relevant government and project leads within one day of discovery.

5.2.10 Develop and provide testing results to the Government Technical POC (TPOC), and project leads, after testing is complete (all or some of these activities may be automated). Upload to SharePoint within 2 business days of completion. This ensures QA is completed with testing and the application is ready for the stated environment (e.g., production or contractor test). At a minimum, results shall include:

- Reference to release (e.g., application and version number)
- Scope of current release (to clarify what the testing focused on)
- Type of testing conducted (e.g., regression, smoke, etc.)

- Total number of test cases, number and percent Assessment of failed or un-tested cases
- Remaining open issues and corresponding issue tracking number (e.g. JIRA tracking number); includes summary, priority and risk associated with open issues
- User impact of open issues
- Workaround if available with failed cases
- Recommendation of how to move forward (yes, goes to production or no, does not go to production)
- Reference to all testing artifacts (e.g., SharePoint site)

5.2.11 Log and track issues, defects, enhancements, etc., found during testing via the DMDC provided issue tracking and reporting system within 2 business days of discovery. Report and communicate issues found to the relevant government and project leads within one day of discovery.

5.2.12 Provide evaluation and testing support for the RAPIDS Platform Support (RPS).

5.3. Test Data Management

5.3.1 Adhere to personally identifiable information (PII) regulations in accordance to DMDC guidelines and all requirements included in the base EITS II contract.. No operational, security-relevant, or personally identifiable information (PII) shall reside within any system or software during development test data maintenance, or QA testing.

5.3.1.1 Ensure all QA test or stub data supporting QA testing and validation is compliant with existing DMDC guidelines for personally identifiable information (PII).

5.3.1.2 Ensure that any PII level test data discovered within historical QA test data is de-identified per DMDC PII guidelines.

5.3.1.3 Assure test data is up-to-date, current and relevant for appropriate use in application. Use existing DMDC approved tools for test data creation and management.

5.3.2 Develop automated test scripts to perform setup of test preconditions, execute functional tests, report results of actual versus predicted outcomes, and other test control and test reporting functions.

5.3.3 Prepare and deliver Integrated Development Package (Design Documents, ETL Scripts, Software Source Code, Test Scripts).

5.3.4 Ensure standardized test cases are developed to be leveraged across other DMDC Enterprise projects. Examples of standardized test suites may include: authentication, log-in, log-out, application monitor health checks, etc.

5.3.4.1 Update and maintain QA testing suites supporting the development and execution of functional tests, the comparison of actual outcomes to predicted outcomes, the setting up of test preconditions, and other test control and test reporting functions when necessary.

5.3.5 Automate new test cases. Exceptions shall be documented and approved by the Government Program Manager and the exception sign off sheet shall be maintained in SharePoint. Exceptions shall follow the process outlined in Appendix M. Automation shall provide efficiencies on the testing cycle duration.

5.3.6 Test cases for new web-based applications shall be written using headless browser libraries. The web-ui automation shall be headless.

5.3.7 In instances where database connectivity is not required for the application, data required for test execution should be serialized to JSON or XML file in order to ensure reliability of environment and results.

5.3.8 Data that must reside in a database for test completion shall be stored and configured in the following ways:

- Stored in such a way that other applications cannot impact the integrity of the data prior to or during test execution,
- Configured so that multiple, asynchronous test automation sessions can be executed for a given application at any given time, and
- Configured using a script, rather than manually, so as to improve efficiency.
- Web-based testing validations shall utilize RESTful endpoints (versus UI activity flows).

5.3.9 Test case code reviews shall be performed periodically by automation engineer leads.

5.3.10 Full code review shall be performed for all new test cases developed.

5.3.11 Maintain automated test cases within Redwood HQ.

5.3.12 Ensure test results include automated alerts for test case failures or when test case execution takes longer than the predefined critical limit. The predefined critical limit shall be that all test case failures generate an alert (typically found in test result reports/logs). If it is determined by the project team responsible for delivering the solution to a DMDC customer, and that customer has determined that failure of a particular test should not prohibit release of the application or feature, then an exception may be applied

5.3.13 The target objective is for less than 5% of automated test cases to fail during automation execution. For each executed automated test suite, the target objective is for less than 5% of automated test cases to fail.

5.3.14 Provide detailed report and business/ technical justification of test cases that must remain manual. The exception process and criteria for manual test cases are outlined in appendix M.

5.3.14.1Test cases deemed not automatable (as approved by the government outlined in Appendix M) shall be tracked as part of the total test cases maintained, but excluded from the automation percentage calculations.

5.3.15 Fifty percent of all applications supported by Enterprise QA shall be 100% automated and executable in the DevOps process, per the guidelines of this task order, by the end of the period of performance.

5.3.16 Provide a monthly metric of Manual Test Cases to include: the total number of test cases, broken out by application, the number of manual test cases, the number of automated test cases, and the month the test cases were moved to the DMDC approved test data management tool.

5.3.17 Report a monthly metric of Automated Test Cases, to include: the number of test cases automated per month, the number and identified applications that has attained 100% automation, total manual and automated test cases per application, failed automated test cases and percent of failure, and the tool the test case is maintained in (e.g., Redwood vs. Mater). All test cases for applications that have been released in the past two years will be included in this metric calculation.

5.4 Test Tools and Automation Frameworks

5.4.1 Maintain and support QA test tools and frameworks currently deployed in the DMDC environment; this includes upgrades as necessary. Testing tools may change during the life of this task

order.

5.4.2 Ensure Redwood HQ provides quality and accurate automated testing; this includes providing updates and maintenance.

5.4.2.1 Maintain the process that identifies: automation failures, the reason for failure, and the required fix for the failure.

5.4.2.1.1 Correct failed automated test cases before next release to production.

5.4.2.2 Maintain the JIRA dashboard to track effort and provide high value metrics. At a minimum, the dashboard shall provide statistics on the following issues: time to resolve, number of open, in-progress, closed.

5.5 Personnel Security Assurance (PSA) Architecture Quality Assurance Support (OPTIONAL CLIN)

In addition to requirements listed in sections 5.1 through 5.4 above, the contractor shall provide the following specific tasks to Conduct extensive QA testing on the DISS Family of Systems (FoS), which includes both Case Adjudication Tracking System (CATS) and Joint Verification System (JVS). The Government expects a consistent level of support as compared to the previous 12 months.

5.5.1 CATS is currently operational at FT Meade; however, DMDC is establishing a Disaster Recovery site within the DMDC infrastructure. CATS also has several upcoming releases approved by the stakeholders to include: a consolidated application, suitability expansion, and feature enhancements.

5.5.2 JVS is currently in development and will require a substantial amount of testing prior to achieving Initial Operating Capability (IOC).

5.5.3 The QA testing and resulting deliverables for both CATS and JVS shall meet the established standards for Acquisition Category III (ACAT III) programs.

5.5.4 Perform ETL activities as required for DISS.

5.5.5 Update and maintain the DISS test tool, user interface (UI), and test database.

5.5.5.1 Maintain documentation and maintenance procedures for the test data tools and processes.

5.5.6 Create and load test data to populate the test database based on input parameters.

5.5.6.1 Create and maintain training material for use of test data creation system and processes (DISS).

5.5.7 Maintain the plan for analyzing the test results for development releases.

5.5.7.1 Maintain a plan describing test data support required for agile development vendors.

5.5.8 Lead Government testing scenarios, capture results, and provide Test Analysis Reports outlining results, defects, severity and resolution.

5.5.8.1 Conduct Government Acceptance Testing (GAT) for each agile development cycle. Provide full regression testing as directed by the Government.

5.5.8.2 Conduct End User Evaluation (EUE) testing with various stakeholders to DISS releases as required by the Government.

5.5.8.3 Reconfigure test data application to support DISS development testing.

5.5.8.4 Update Test Data application to create test data to support interface testing and application testing.

5.5.8.5 Update Database creation scripts to populate data tables in DISS data model

5.5.9 Follow and support the practices and configuration management processes as outlined in the DISS Technical Guidance Document (TGD) and DISS Configuration Management Plan (CMP).

5.5.10 Test and verify tools and processes in accordance with the processes documented in the DISS TGD, to ensure that the test data tools provide outputs that mirror production data. The test data creation tool outputs will also be integrated in the same manner as the production data. The contractor will use automation where appropriate to minimize human intervention when using the test data creation tools and processes.

5.5.11 Provide support for the test tools that were created to generate the test data. This effort will include problem resolution and maintenance. The contractor shall refer to the DISS TGD for support specifications.

5.5.12 Prepare and deliver Analysis and Design Document.

5.5.13 Create documentation and reference materials for development releases

5.5.13.1 Coordinate and provide materials for training development

5.5.13.2 Provide DISS screenshots with test data for training materials

5.5.13.3 Create test data based on input and workflow status for training scenarios as requested by the Government.

5.6 Migrate automated test cases from internal tools (e.g., "Mater") to the DMDC approved test data management tool (OPTIONAL CLIN)

The current number of cases automated in legacy tools are approximately 26,000

5.6.1 Migrate all web services automated test cases from non-approved internal tools to the DMDC approved test data management tool.

5.6.2 Migrate all batch application automated test cases from non-approved internal tools to the DMDC approved test data management tool.

5.7 Provide a Thick-Client Solution for Automation (OPTIONAL CLIN)

5.7.1 Implement the Desktop Automation Tool (DAT), to include integration of the DAT, to include set up, configuration and training.

5.7.2 Configure and implement the thick client environment.

5.8 DMDC DISA Data Center Migration (OPTIONAL CLIN)

It is anticipated that all applications supported at DMDC will migrate to the DISA Data center.

5.8.1 QA shall conduct smoke testing on applications that have migrated to the DISA Data Center to ensure applications run as well as or better than the current production version.

5.8.2 QA shall coordinate with project teams to ensure the appropriate smoke tests are executed to provide confidence the application runs as expected.

5.8.3 All applications that DMDC supports and moves to DISA shall be tested.

5.8.4 Maintain QA specific project plans required to support government initiated initiative.

5.9 508 Compliance (OPTIONAL CLIN)

5.9.1 Execute 508 compliance audit, utilizing DMDC provided COTS product. Follow and maintain the 508 compliant standard operating procedures (SOP) in Appendix B. The purpose of the audit is to assure applications are compliant with 508 standards as set by the United States Access Board.

5.9.1.1 Document results in 508 dashboard, located on SharePoint, within 2 business days of completion.

5.9.1.2 The government anticipates no more than 15 audits shall be conducted.

5.10 Service Validation and Testing (OPTIONAL CLIN)

There will be government support for this tasking to include a government process manager, owner and champion.

5.10.1 Consult with the business process realignment (BPR) team regarding QA business processes, SDLC, releases, and KPI to the government and/or other contractor support personnel for creating or updating of BPR documents.

5.11 Electronic Health Record Management (EHRM) Testing (OPTIONAL CLIN)

5.11.1 5.11.1 Provide Quality Assurance Support for Electronic Health Record Modernization (EHRM) Applications This CLIN shall follow the requirements listed in sections 5.1 through 5.4 above. The Government anticipates a mix of major, minor, and maintenance releases for up to 6 of the 12 applications. The government anticipates a consistent level of support as compared to the previous 12 months. **NOTE – EHRM QA support is NOT included in the estimated release counts listed under PWS Section 3.2 above**.

5.12 Physical Security and Law Enforcement Applications (PSLE) Testing (OPTIONAL CLIN)

5.12.1 Provide Quality Assurance Support for PSLE applications. The Government expects a consistent level of support as compared to the previous 12 months. **NOTE – PSLE QA support is NOT included in the estimated release counts listed under PWS Section 3.2 above.**

5.13 Provide Quality Assurance Support for ACTUR Applications

5.13.1 This CLIN shall follow the requirements listed in sections 5.1 through 5.4 above. The Government anticipates a mix of major, minor, and maintenance releases for up 19 releases

5.14 Provide Quality Assurance for Accountable Car Organizations (ACO) Demonstration

5.14.1 For the ACO Demonstration the contractor shall provide a one major release with multiply release items. The release shall focus on enrollment fees and the PCM business areas. Note: ACTUR QA support is NOT included in the estimated release counts listed under PWS Section 3.2 above.

5.15 REPORTS AND MEETINGS

5.15.1 In-Progress Review (IPR).

The Contractor shall follow the IPR requirements identified in the PWS Section 5.8.5 of the EITS II Base IDIQ

5.15.2 **QA Dashboard**

Contribute to maintenance of a QA Dashboard to provide visibility into QA functional activities including the metrics, QA testing workloads, automation coverage in applications progress, escape metrics, and enterprise QA initiatives. The contractor will collaborate with other DMDC functional groups as necessary including change, configuration, release management, and project leads to incorporate existing data as applicable to the QA Dashboard. This dashboard shall remain available to the government on SharePoint.

5.15.3 **Monthly Status Reports (MSR) and Senior Management Review (SMR)**

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

5.15.4 Problem Notification Reports

The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.0 Deliverables

All deliverables and work products shall be submitted to the COR in electronic format for acceptance and approval. The acceptance of deliverables and satisfactory work performance shall be based on the timeliness, accuracy and standards as specified in the requirements of the PWS.

Deliverable	PWS Reference	Delivery Date
Quality Management Plan Update	5.1.1	Within 15 days of award
Automation Project Plan Draft	5.1.2	Within 15 days of award
Automation Project Plan Final	5.1.2	Within 30 days of award
QA Test Strategy	5.1.3	Within 30 days of award
Monthly Metrics	5.1.4	Monthly with SMR
Defect Report	5.1.5	Monthly with SMR
Updated Staffing Plan	5.1.7	Within 10 days of award; updates within 5 days of change
IPR Minutes	5.1.10	Within 3 business days of meeting
Quality Control Plan	5.1.11	Within 10 days of award
Risk Management Plan	5.1.12	Within 10 days of award
Requirements Traceability Matrix	5.2.5.1	Updated throughout development lifecycle
Test Transaction Reports	5.2.8.1	Conclusion of testing; available upon request
Test Results	5.2.11	Within 2 business days of testing completion
Manual Test Case Report	5.3.16	Monthly with SMR
Automated Test Case Report	5.3.17	Monthly with SMR
Dashboard Report	5.10.13	Monthly with SMR
SMR Slides	5.10.13	15th of each month
SMR Notes	5.10.13	Within 3 business days of SMR
Kickoff Notes	8.4	Within 3 business days of meeting

7.0 QUALITY SURVEILLANCE

The Government may follow the Appendix P - Quality Assurance Surveillance Plan) to EITS II IDIQ Base Contract

7.1 Contract Discrepancy Report (CDR).

The Contractor shall follow the requirements identified in PWS Section 5.8.8 of the EITS II Base IDIQ

7.2 Problem Notification Reports (PNR).

The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

7.3 Performance Standards and Acceptable Quality Levels

QA Specific Performance Objective	QA Specific Performance Threshold
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.

Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.
QA Specific Objectives	5.1.4 Provide the percentage of test case execution per release. Unless otherwise agreed upon with the government COR, test case execution shall be 100% for all project releases. Provide on the signoff documentation to project teams. % of test case execution (indicates the progress of testing by giving the percentage of test cases executed with the result of a pass, fail, or blocked result) Percent of Test Case Execution = (Number of Passed Tests + Number of Failed Tests + Number of Blocked Tests) / Number of Test Cases
	5.1.4 Provide defect leakage rate. Rate shall remain at 5% or less per release. Report progress in SMR. Defect Leakage (used to identify the efficiency of the QA testing) = (No. of Defects found in UAT and Production per release/ No. of Defects found in QA testing per release) * 100
	5.3.13 The target objective is for less than 5% of automated test cases to fail during automation execution.
	5.3.5 Applications automated at 100% shall be at least 50% more efficient than the baseline testing cycle. The percentage may be adjusted if there are test cases that cannot be automated, per the government guidance provided.

	5.3.15 • Within 3 months, 15% of applications shall be 100% automated • Within 6 months, 25% of applications shall be 100% automated • Within 9 months, 35% of applications shall be 100% automated • By end of the task order, 50% of applications shall be 100% automated Baseline measurement: Assumes the number of applications is based on the release count identified in PWS Section 3.2 at time of award.

QA Dashboard will be used a surveillance method for the above discussed metrics.

Positive Incentives: Past Performance Evaluation

Disincentives: The Government will request considerations of the metrics are not met.

8.0 Contract Administration.

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

8.1 Contract Type: This contract type of firm fixed price

8.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award.

8.3 Place of Performance/Hours of Operation: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section 9.0- Travel.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m depending on their physical location. Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

8.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ

8.5 Points of Contact:

DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. James Purdy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: James.Purdy@gsa.gov
Tel: 215-514-3952

GSA Contract Specialist (CS)
Mr. Rajdeep Singh
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: rajdeep.singh@gsa.gov
Tel: 215-446-2868

GSA Contracting Officer's Representative (COR)
Mr. Ruslan Gorbonos
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Ruslan.Gorbonos@gsa.gov

Tel: 215-446-5820

8.6 Government Furnished Property/Equipment/Information (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ

8.7 Travel: Local or long-distance travel may be required to various locations CONUS. The annual travel estimate is $5,000.00. The Contractor shall follow the travel requirements identified in Section 10.7 of the EITS II PWS.

8.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ

8.9 Inspection, Acceptance, and Payment: The Contractor shall follow the IPR requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ

8.10 Invoicing: Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

9.0 APPENDICES

Appendix A – Product Roadmaps

Appendix B – 508 Processes and Procedures Guidelines

Appendix C – Description of Sample DMDC Projects

Appendix D – Description of Environments

Appendix E – Test Plan Sample Template

Appendix F – QA Tester Handbook

Appendix G – Requirements Traceability Matrix Overview

Appendix H – Glossary for QA Task Order

Appendix I – QA Process Workflow

Appendix J – Template Checklist

Appendix K – Template QA Test Sign Off

Appendix L – QA Process Workflow Checklist

Appendix M – Automation Exception Process

Appendix N – Historical QA Workload 2017-2018

ASSIST Order ID No: ID03180056003
GSA/FAS Mid-Atlantic Region

Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Defense Biometric Identification System (DBIDS) and Identity Matching Engine for Security and Analysis (IMESA) Support
ORDER ID - ID03180056003

1.0 INTRODUCTION

The Defense Manpower Data Center requires Subject Matter Expertise (SME) and Program Management support for the Physical Security and Law Enforcement program to include Physical Access Control Systems (PACS), Defense Biometric Identification System (DBIDS) and Identity Matching Engine for Security and Analysis (IMESA).

2.0 BACKGROUND

2.1 Military installations across the Department of Defense (DOD) utilize outer and inner perimeter rings with varying levels of security to control physical access to secure areas. The Defense Biometric Identification System (DBIDS) Business Rules Committee (BRC) has requested that DMDC analyze the architecture of the current Base Services and/or totality of the DBIDS 5 application in managing identities and their respective unique profiles. DMDC will work with the BRC to facilitate the execution of the requirements referenced in this document. The enterprise goal is to integrate these findings with DBIDS for optimization and data quality. This new solution must be cost effective and provide a scalable approach that can be implemented across the DOD enterprise and identified in future development roadmaps.

2.2 DMDC supports major programs and initiatives within the DOD and maintains the largest archive of personnel, manpower, training, security and financial data within the DOD. Specifically, DMDC's data supports decision making to determine the eligibility for both physical and logical access to military installations and DOD systems worldwide. DMDC's physical and logical access systems include the Defense Biometric Identification Service (DBIDS) system which identifies DOD affiliated persons through the use of ID cards, base passes, and biometric attributes and grants access based on their privileges in accordance with their purpose, fitness and status.

2.3 DMDC has developed the Identity Matching Engine for Security and Analysis (IMESA) physical security concept, designed to continuously evaluate the fitness of persons who have attempted and are attempting to access DOD installations. The IMESA solution uses DoD, Federal, State, and local authoritative data sources to look for derogatory information and send alerts to authorized and connected Physical Access Control Systems (PACS) so individuals who may pose terrorist, criminal, and/or security threats may be detained and adjudicated. The IMESA solution covers all DoD installations and any person seeking to gain physical access to them and enhances the security of DoD personnel. Personnel data in the IMESA solution comes from two places: the Defense Enrollment Eligibility Reporting System (DEERS) and the Local Population Database (LPDB). IMESA pulls from DEERS information on individuals who possess credentials authorized to facilitate access. The LPDB provides the IMESA solution with data on individuals who possess a credential authorized to facilitate access to installations that are not contained in DEERS; this includes non- DoD Federal Personal Identity Verification (PIV) credentials, approved DoD PIV-Interoperable credentials, local DoD installation issued

cards/passes, Transportation Worker Identification Credentials (TWIC), Veteran Health Identification Card (VHIC) and other authorized credentials.).

3.0 SCOPE

The Contractor shall provide the personnel and management necessary to support planning, designing, sustaining, developing, and implementing Physical Security and Law Enforcement (PSLE) programs and systems.

4.0 REQUIREMENTS

The Contractor shall:

4.1 DBIDS Sustainment Development

The contractor shall provide the personnel and support necessary for development of all current product services and continue integration into DBIDS 5 (D5), and also provide documentation and creation of training material, processes, and procedures in support of the requirements in Section 4. The contractor shall be responsible to create/sustain/maintain a production integration system that can handle all D5 services as defined by the D5 Roadmap and approved requirements.

4.1.1 Product Enhancement

4.1.1.1 Maintenance of Existing Applications

4.1.1.2 Support the software maintenance of all portions of the D5 and IMESA software applications to include the following:

- Routine and emergency bug fixes
- Routine software changes caused by dependent third-party library updates
- Minor software changes caused by policy changes
- Depending on number of components requiring updates, per approved project plan

4.1.1.3 Support the update and refinement of features as maintained in the government approved business requirements.

4.1.1.4 Utilize most current approved requirements documentation at the start of the Period of Performance. (Government furnished).

4.1.1.5 All software changes to D5 will be confirmed in a production staging environment with participating beta installations for a period of no less than 14 days before being pushed to production except for an emergency, a Change Request shall be approved, signed off via email and directed by the government.

4.1.1.6 Confirmation (e-mail with documentation) shall include a confirmation of data integrity between CONUS DBIDS, IOLS, and PDR, at a minimum, and sign off from DBIDS and IMESA Government Product and Program Managers.

4.1.2 Reports

4.1.2.1 Investigations Report

Contractor shall develop a report to display all personnel who have generated a dossier on a particular individual. Report user shall be able to search for report by requesting operator or by investigation subject via DBIDS ID. Report shall detail the where the ORI (Originating Agency Identifier) was requested from and the timestamp the report was generated. Report shall not be restricted by date range. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.2 Operator Transactions Report

Contractor shall develop a report to display a list of operators who have scanned at the local installation and sort them by number of transactions recorded. The guard scans shall be grouped by base and ACP (Access Control Point). The report shall show the total per guard, base at which they are scanned, then total scans per base. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.3 Installation Health Report

Contractor shall develop report to display usage rate of issuances compared to scanned frequency, and other health metrics. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.4 Issuance by Operator Report

Contractor shall develop report to display all credentials issued by a particular operator at an installation. The following fields shall be returned after report is generated: operator, credential type, and total. Report shall be filterable by date range, base, and credential type. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.5 Enhanced Screening Watch list Reports

Contractor shall develop report to display events and remarks from the Enhanced Screening Watchlist within a given date range. The following fields shall be returned after report is generated: subject name, photo (if exists), address, email, identifier, aliases, any remarks, and total event history. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.6 Base Access Control Report by Credential Type

Contractor shall develop report to display scans at a base grouped by credential type within a given date range. The following fields shall be returned: date, name, direction, access decision, reason, action, operator name, and credential type. The report shall show a total number of each in the header of report. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.7 Exception to Policy (ETP) Report

Contractor shall develop report to display all instances where an ETP was applied to an individual. This report shall be base specific and ETPs applied will be grouped by operator who applied the ETP. The following fields shall be returned when the report is generated, date the ETP was applied, subject of ETP's name, any remarks associated with ETP status, begin date and end date of ETP status, and total number of each in the header of report. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.8 Vetting Adjudication Aggregate History Report

Contractor shall develop report to display adjudications by aggregate (approved, denied, and access type) over a date range. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.2.9 Forecast Re-adjudication Report

Contractor shall develop report to display individuals who will need to be re-adjudicated within a certain date range (30, 60, or 90 days). The report will be timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.1.3 Data Warehousing

Contractor shall build out an initial Data Warehouse in Structured Query Language (SQL) Server Analysis Services.

- Contractor shall build out star schema using fact and dimension tables for the access transaction data. The contractor shall conduct analysis on what fact and dimension tables need to be created.
- The Contractor shall create SQL Server Integration Services jobs to migrate data from online transaction processing (OLTP) to the Online Analytical Processing (OLAP).

4.1.3.1 Enhance SQL Server Reporting Services (SSRS)

Contractor shall modify the enrollment workstation and web portal to be compatible with dynamic SSRS reports. Contractor shall build out enhanced SSRS environment.

4.1.3.2 Power Business Intelligence (BI)

Contractor shall conduct analysis on whether Power BI would be usable in a DOD production environment to give Service points of contact enhanced business intelligence capabilities.

4.1.4 Base Service Modeling and Performance Enhancements

Contractor shall fix technical debt acquired from legacy DBIDS components remaining from data migration, and old versions of IMESA. This is necessary to deliver new features and resolve DMDC mandated cybersecurity/security/coding compliance issues going forward.

Specific areas to fix are:

- Sponsorship for base access instead of sponsoring credentials
- Consolidation of credential models
- Access permissions applied to the individual rather than affiliation

4.1.5 Facial Recognition

4.1.5.1 Contractor shall implement functionality during enrollment at the registration workstation to use facial recognition as a way to assist in the disambiguation of potential matches of biographic data.

4.1.5.2 Contractor shall implement functionality to allow a credential to be scanned, pull up the latest picture on file in DBIDS or IMESA / Defense Enrollment Eligibility Reporting System (DEERS) and determine if the person presenting the credential at the registration workstation matches the photo on file.

4.1.6 Vetting Module

4.1.6.1 Contractor shall integrate IMESA real-time queries and display eXtensible Markup Language (XML) returns. Due to historical IoLS identity limitations, there are often multiple IoLS profiles for a single

person in DBIDS. This will allow the vetting officer to determine if there are any statuses that are not being merged and take appropriate action.

4.1.6.2 Contractor shall assist Government in determining feasibility of integrating with NCIC-CE (National Crime Information Center – Continuous Evaluation).

4.1.6.3 Contractor shall assist Government in determining feasibility of integrating with JPAS/JVS (Joint Personnel Adjudication System/Joint Verification System), Interpol, DCII (Defense Central Index of Investigations), and other DBIDS regions.

4.1.7 Identity Proofing Module

4.1.7.1 Contractor shall add identity breeder document capture in workstation and integrate with Government designated document scanner once determined.

4.1.7.2 Contractor shall perform a proof of concept on 10-print live scan.

4.1.7.3 Integrate NLETS (National Law Enforcement Telecommunications System) driver's license query and passport query by displaying the XML return by NLETS.

DBIDS Additional Development (OPTIONAL)

4.2.1 Mobile Enrollment and Credentialing (OPTIONAL)

4.2.1.1 Upon execution of OPTIONAL CLIN, the Contractor shall have 12 months to implement core infrastructure to support a multiyear effort to implement a secure, multi-platform mobile enrollment and credentialing system detailed below under 4.2.1.

4.2.1.2 Develop and Maintain Sponsor Website.

- The sponsor website shall allow an authorized user to send invitations for installation access and provide preliminary identity proofing of the invitees.

4.2.1.3 Website Authentication

- The website shall require Common Access Card (CAC) authentication for users affiliated with the DOD, Personal Identity Verification (PIV) authentication for users affiliated with another U.S. government agency, and email/password for DBIDS card holders.

4.2.1.4 Access Invitations

- The sponsor shall have the ability to send a single access invitation consisting of invitee name, email address, mobile phone number (optional). The sponsor must include the name of the installation, where access is needed, the date range access is required, and a reason for access or comments text block.
- The sponsor shall have the ability to send an event or group invitation (e.g. Basic Military Training invitee list). The invitation must include a group/event name, the name of the installation where access is needed, the date range access is required, a reason for access or comments text block, and one or more invitees which shall consist of name, email address, and mobile phone number (optional).
- Upon sponsor submission of the invitation, the system shall send out an email and an optional text to the invitee containing instructions on how to start the enrollment process. The email shall

contain a link that, when opened on a mobile device, shall redirect to the appropriate app store to download the DBIDS Mobile Credential App.

- If the invitee is already known to the system, the system shall additionally send a notification to the DBIDS Mobile Credential App on the invitee's phone.

4.2.1.5 Invitee Identity Proofing

- Once the invitee(s) a sponsor has invited have finished their mobile enrollment, the sponsor shall be notified (by email, optionally text, and within the Sponsor Website) that he needs to verify the invitee's identity.
- The sponsor shall view the invitee "selfie" photo taken and confirm, deny, or indicate he is unsure whether the photo matches the person invited.

4.2.1.6 Mobile Credential.

- The mobile credential application shall be used for identity enrollment into DBIDS and, upon a positive adjudication by a vetting officer; it shall be used as an access credential. The token for the access credential shall be derived using a one-time password (OTP) algorithm.
- The mobile credential must operate on both iOS and Android devices.
- Authentication
    - The mobile credential user shall have the option to authenticate with email/password, Facebook ID, or Google ID (including Facebook and Google would help with identity proofing).
- Account
    - The user must setup an account that is tied to the email address provided by the sponsor.
    - The user must verify possession of the email address used by clicking on a link in an email where the link contains a temporary token that ties back to the account created.
    - During account creation, the user may select whether to use an email/password, or acceptable single sign on methods as an authentication mechanism.
    - The user can select to enable Touch ID, Face ID, or Pin for subsequent logins on that mobile device.
- Enrollment
    - The user must start the enrollment process by capturing their face from multiple angles.
    - The software shall use facial detection software to ensure that appropriate data is collected.
    - The user must enter a primary identifier number per the DBIDS system requirements.
    - The user must take a photo of the front and back of his primary identify proofing credential. This is limited to REAL ID (i.e. Government ID, Standard driver's license, etc) or Passport.
    - The software shall extract the user's name, date of birth (DOB), aliases, and address from the credential.
    - The software shall extract the face photo from the identity proofing credential provided and send both that photo and the mobile capture photo to a web service. The web service shall perform facial recognition between the two photos and determine if the person is the same.
    - The user must take a photo of the front and back of a secondary proofing document.
    - The user shall have the option to manually enter his name, DOB, address(es), phone #('s) if that information could not be captured via the credential scan.
    - If the identity information is entered manually, the system must extract identity information from the primary and secondary proofing document using OCR, and ensure that the 3 identity sources match.
    - The software shall maintain an event log of all actions performed during the enrollment.

- The software shall submit the user's completed enrollment to the sponsor and vetting officer for additional proofing and vetting.

4.2.1.7 Identity Services

4.2.1.7.1 Facial Recognition

- The identity web service shall accept a photo of a credential containing a facial photo and a photo of a person, perform facial recognition between the two photos, and return a match result.

4.2.1.7.2 Counterfeit Credential Detection

- The identity web service shall accept photos of REAL ID and Passport credentials and use machine learning/AI to detect a counterfeit.
- In order to perform the machine learning, a training set of the supported credentials (valid and invalid) must be generated / acquired.

4.2.1.7.3 DBIDS Identity Matching Engine

- The identity web service shall run each identity profile against an identity matching algorithm to ensure the profile does not already exist in DBIDS. The algorithm shall include the following:
  - Diacritic characters shall match to their base glyphs (e.g. ä matches a, ĉ matches c)
  - String similarity matching using the damerau-levenshtein algorithm (to catch minor misspellings).
  - Address matching.
  - Identifier matching.
  - Biometric matching (fingerprints, iris, facial).
  - Alias name matching.
  - Email matching.
  - Phone number matching.
  - Common nickname matching (i.e. Richard with also match on Rick, Rich, etc. even though those aliases were not provided).
  - Each match shall receive a score from 0 to 100.
  - Each matching category shall receive a weight.
  - The identity matching engine shall return a weighted score based on the comparison between the two identity profiles.

4.2.1.8 Mobile Enrollment and Credential Validation

- Contractor shall work with stake holders to identify and document additional requirements necessary to complete follow-on work required for full implementation of mobile enrollment and validate and confirm mobile credential information.

4.2.2 IdAM(Identity Access Management) Solution (OPTIONAL) - Upon execution of OPTIONAL CLIN and acquisition of IdAM solution the Contractor shall have 12 months to implement the IdAM solution.

4.2.2.1 Any changes identified by the Government shall require the Contractor to determine changes to requirements, costing model, and potential conflicts with previously proposed solution, and added to the approved project plan.

4.2.2.2 The IdM (identity management) solution shall monitor the regional DBIDS database and upon the detection of an operator account being created, shall start an in-processing workflow. The IdM solution shall be the platform for in-processing, provisioning, account maintenance, continuous evaluation of, and out-processing for DBIDS users in order to stay compliant with account lifecycle management policies.

4.2.2.3 This solution shall satisfy the two-factor authentication requirement mandated by DoD.

4.2.2.4 This solution shall enable the transition to the PIV-Auth cert as mandated by DoD.

4.2.2.5 The IdM solution shall monitor the regional DBIDS database and upon the detection of an operator account being created, shall start an in-processing workflow.

4.2.2.6 The in-processing workflow shall consist of DD-2875 workflow which involves the user's supervisor and a government approver.

4.2.2.7 Upon approval of the 2875, the account shall be provisioned into Active Directory and other supplemental DBIDS user stores.

4.2.2.8 Additional in-processing workflows can be requested by Government and requirements be established by Contractor.

4.2.2.9 Contractor shall provide access to Government requested users to provide auditing and governance of 2875s.

4.2.2.10 The IdM solution shall continuously monitor the regional DBIDS database for any adverse statuses or account termination requests and if detected, shall start an out-processing workflow.

4.2.2.11 The out-processing workflow shall consist of disabling the user's account in Active Directory and any other supplemental DBIDS user stores.

4.2.2.12 The IdM solution shall implement a bulk processing task to transition all user accounts from a DoD identity cert authentication to the PIV-Auth cert.

4.2.2.13 All DBIDS application authentication shall be consolidated to use the IdAM solution access manager.

Device Configuration Updates (OPTIONAL)

4.2.2.14 Contractor shall augment to include ability for hardware middleware, access control devices, and ACWs (Access Control Workstations) to communicate back to a web service hosted at the regional data center and write execution context information.

4.2.2.15 Contractor shall create a report that displays the connectivity status of the various devices stated above. The report shall be grouped by base. The report will have a generation timestamp in a non-invasive location. There shall be an export button with option to export the entire report to .csv.

4.2.2.16 Contractor shall create a method for setting the configuration values such as mapping the IP address to ACP (Access Control Point) Mapping, Gate assignment, timeout values, access code settings, etc.

4.2.2.17 This method should accommodate the following Access Control Devices: Lantronics, iCam7, enhanced secure pedestrian gate (ESPG), and the Cheetah AVG.

4.3 **IMESA Enhancements**

4.3.1 Provide development support based on policy updates provided by DMDC, OUSD(I) and other stakeholders.

4.3.2 Develop tool for internal use to visualize all relevant information of an individual based on LPEDI or DoD EDI

4.3.3 Review existing ICD (Interface Control Document) and propose changes to government stakeholders on a quarterly basis in a formal report with proposed changes.

4.3.4 DBIDS integration development with IMESA changes will occur per approved project plan.

4.3.5 Add an error for partial ADR (Active Data Repository in DEERS) information on inquire by identity when DOB is missing

- Add an indicator to display a person status
- *Add credentials used for registration*
- Allow more than one credential to be added to an identity

4.3.4 Review and report existing architecture to determine where potential data integrity issues could occur based on multiple supported ICDs, multiple PACS (Physical Access Control System), and multiple regions.

4.3.5 Develop standardized method to merge identities determined to be duplicate and expose the necessary information to participating PACS and recommendation to implement their own merge protocols.

4.3.6 Work with government stakeholders to identify policy on exposing additional functionality not documented in the official ICD for beta development and testing purposes by participating PACS.

4.3.7 Add the ability to search all completed cases without the need to load all cases into the GUI

4.3.8 Allow the user with a specific role to select which IMESA application they would like to view (e.g., Dashboard, multi-threat alert center (MTAC), law enforcement officers (LEO)

4.3.9 Create new user roles for the IMESA application, IMESA Managers and LEO roles

4.3.10 Update Matching Algorithm

4.3.11 Allow PACS to confirm receipt of data alert when needed

4.3.12 Build a LEO application for external users

4.3.13 Develop functionality allowing users to export Dashboard reports to Excel

The following paragraphs apply to the sections that immediately follow regarding terrorist screening database (TSDB) Phase II, national sex offender registry (NSOR) Integration, violent person file (VPF) Integration, and interstate identification index (III) POC:

4.3.14 The research and development for the NSOR and VPF will proceed in parallel with the research for the III, and each can succeed independently. This parallel structure is necessary given the greater level of risk associated with the III research compared with the NSOR and VPF.

4.3.15 The Initial Capabilities Document development and Interoperability Layer Service (IoLS) development are two sequential tasks that will also proceed in parallel with the NSOR and VPF, but which must complete prior to the NSOR and VPF completing.

4.3.16 The TSDB portion requires technical work such as identity resolution / matching, database design, software development, website development, PKI-enablement, workflow processing, technical writing, and program management.

4.3.17 TSDB Phase II

- Contractor shall build upon the work done in the previous phase by making minor enhancements to the TSDB match review capability and implementing person-oriented reporting for NCIC-origin security alerts, researching and developing a way to eliminate duplicate alerts for the same person and offense as present in current alert-based reporting. Contractor shall research applicable criminal justice regulations to ensure that this reporting is implemented in accordance with the same.
- Contractor shall test all enhancements in accordance with TSDB testing rules, and the reports submitted to the Government. The granular reporting functionality will be spot checked by having two installations manually tally the results of their security alerts and matching those tallies against the generated report.

4.3.18 NSOR Integration

- Contractor shall design and develop the required enhancements to the IMESA matching engine workflow to identify potential matches between all registered cardholders and the NSOR with varying degrees of data quality and match points.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of NSOR originated alerts to the Installations.
- Contractor shall develop a capability to transmit alerts derived from changes in person data from NSOR through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.19 VPF Integration

- Contractor shall design and develop the required enhancements to the IMESA matching engine workflow to identify potential matches between all registered cardholders and the VPF with varying degrees of data quality and match points.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of VPF originated alerts to the Installations.
- Contractor shall develop a capability to transmit alerts derived from changes in person data from VPF through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.20 III POC

- Contractor shall design and develop a capability to monitor and provide alerts for any changes in III data on all registered cardholders. Contractor shall coordinate with the FBI, criminal justice information system (CJIS), and related groups and boards as necessary to research and design this process.
- Contractor shall make the required updates to the Interface Control Document that describes the technical underpinnings of the interface between the installation physical access control systems and IMESA to support the transmission of III originated alerts to the Installations.

- Contractor shall develop a capability to transmit alerts derived from changes in person data from III through IoLS to the IMESA-connected PACS, including IMESA's ability to receive, through loLS, any necessary PACS acknowledgements of those alerts.

4.3.21 DoDM 5200.08, Vol 3

- Contractor shall implement changes required per DoDM 5200.08, Vol 3.

4.4 IMESA Integration with DBIDS

4.4.1 DBIDS shall be the system used for initial demonstration of any modifications to IMESA.

4.4.2 DBIDS integration development with IMESA changes will occur per approved project plan.

4.4.3 Except in the event of an emergency Change Request, any change to IMESA shall be confirmed in a production staging environment with participating beta installations for a period of no less than 14 days before being pushed to production.

4.4.4 Confirmation shall include a confirmation of data integrity between CONUS DBIDS, IOLS, and PDR, at a minimum.

4.4.5 Confirmation shall include sign off from both product owners - DBIDS and IMESA Government Product and Program Managers.

4.4.6 Integrate TSDB Phase II with DBIDS

Contractor shall implement TSDB Phase II functionality to include the capability of storing silent encounters received from IMESA.

4.4.7 Integrate NSOR with DBIDS

Contractor shall work with Interoperability Layer Service (IoLS) to analyze requirements to demonstrate PACS ability to ingest NSOR data and properly display access recommendation and mitigate concerns from the customer base regarding policy of NSOR data.

4.4.8 Integrate VPF with DBIDS

Contractor shall work with IoLS to analyze requirements to demonstrate PACS ability to ingest VPF data and properly display access recommendation and mitigate concerns from the customer base regarding policy of VPF data.

4.4.9 Integrate III POC with DBIDS

Contractor shall work with IoLS to analyze requirements to demonstrate PACS ability to ingest III data and properly display access recommendation and mitigate concerns from the customer base regarding policy of III data.

4.4.10 DoDM 5200.08, Vol 3

Contractor shall support necessary changes introduced in DoDM 5200.08, Vol 3 by assisting Government in deriving requirements for implementation in DBIDS and IMESA.

4.5 Baseline DBIDS Operations/Production Support (approximately 300 bases/installations connected to the CONUS RDC (Regional Distribution Center)

4.5.1 The contractor shall perform the maintenance and administration of the following items to support the DBIDS and Labs infrastructure as listed below.

4.5.2 Support, maintain and administer the clients, servers and applications as outlined in Appendix 2.

4.5.3 Maintain operating system - Weekly Patching / STIGS / Updates

- Maintain up to date IA approved OS image for future servers

4.5.4 Monitor capacity and performance issues and provide upgrade support and recommendations prior to end of life status.

4.5.5 Review the 5 year planning cycle provided by DMDC for all DBIDS hardware on a semi-annual basis identifying any potential compatibility issues.

4.5.6 Review the 5 year planning cycle provided by DMDC for all DBIDS software dependencies on a semi-annual basis identifying any potential compatibility issues.

4.5.7 Provide business architecture support by ensuring system design diagrams remain up-to-date, update documents and views based on configuration changes, evolving requirements, data flows and security enhancements, use SPARX or other tool as provided by government.

4.5.8 Maintain NoSQL Databases - DBA

4.5.9 Maintain Relational/non-relational Databases - DBA for SQL Relational Database Administration

4.5.10 Perform Data Quality Analysis – Respond to inquiries from Product and Program Managers when there are data quality or data integrity issues that need to be resolved.

4.5.11 Respond/perform Misc. Adhoc Requests - Requests may include: troubleshooting, ACW (Access Control Workstation) for individual installation, networking, OCONUS RDC administration guidance, and other requests outside of Tier 3 helpdesk support. The Government anticipates an average of 30 per year, ad hoc requests from DMDC and its customers. Provide monthly ad hoc report status.

4.5.12 Migration of Training Environment

- Contractor shall facilitate deployment of training environment into identified/approved cloud provider.
- Contractor shall facilitate the creation and administration of Active Directory forest and subdomains as needed.
- Contractor shall facilitate the creation and administration of Windows and Linux servers as needed to deploy the DBIDS stack.
- Contractor shall ensure compliance with all DoD IA STIGS as per FedRAMP+ solution.
- Contractor shall deploy data stores as needed.
- Contractor shall deploy web servers as needed, including load balancers and reverse proxies.

- Contractor shall provide demonstration environment. However, production implementation is dependent on Government licensure.
- Contractor shall deploy any dev required development dependency in order to support the build and deploy pipeline.
- Contractor shall automate the deployment of the software in the training environment using DevOPs pipeline.

4.5.13 DBIDS Monthly Statistics Rollup
Contractor shall provide an updated monthly DBIDS brief with relevant statistics for number of transactions, statuses, dbids credentials and visitor passes created, registrations, etc., as well as, updated application screenshots

4.5.14 Training Material
Contractor shall provide updated Training Material (i.e. User Manuals, Training Manuals, Training Videos) and make available on the DBIDS marketing site and the wiki per government direction.

4.6 DBIDS 5 Worldwide Tier 3 Help Desk

4.6.1 Provide Tier 3 helpdesk support 0800-1700 PST on site in the DoD Center.

4.6.2 Establish and maintain the Tier 3 helpdesk log with problem, date received, estimated completion date and priority. The Government product owner shall assign priorities during the weekly IPR.

4.6.3 All logged items that remain be reported in the monthly SMR and reported to the product owner.

4.6.4 Performance requirement summary for Tier 3

Requirement	Delivery
Triage tier 3 tickets for resolution	2-hours of receipt of ticket
Notify customer of the status of the ticket	4-hours of receipt of ticket
Update root cause of ticket	8-hours of receipt of ticket
75% of all tickets resolved	6-hours of receipt of ticket
100% of all tickets resolved	3-business days

1. Notify Government lead at if unresolved after 3 business days.

2. Provide updates to Government lead as requested.

3. Provide weekly report of Tier III tickets to Government lead to include cumulative status year to date by month.

4. Identify and provide recommendation to recurring issues.

5. Performance requirement summary for Tier 3 is only applicable to tickets received during 0800-1700 PST, Monday-Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The clock for any ticket received outside of these hours will start next business day at 0800 PST.

6. Performance requirements summary apply to tickets once assigned to DBIDS DMDC West Queue (Tier 3).

7. These requirements are applicable to tickets that involve work to be performed by the GCE DBIDS Tier 3 team. Any ticket that requires work to be performed external to the GCE DBIDS team is outside of this performance requirement scope. However, GCE will provide ticket status to Government lead if not resolved within 3 business day and when applicable, continue to provide status within weekly IPR.

4.7 Full 24 hour Regional Distribution Centers (RDC) Support. (OPTIONAL CLIN)

4.7.1 Expands help desk Support to 24/7 coverage in the DoD Center.

4.7.2 Expands help desk Support to include OCONUS RDC system administrative support**.**

4.8 Provide Cyber Security Support

4.8.1 Provide administrative and logistical support for the operations environment of DMDC physical and logical access control systems and applications supporting the DoD goal of strengthening cyber capabilities and expertise to ensure reliability while countering and preventing threats.

4.8.2 Provide technical support to planning, execution, analysis and performance of decision processes, applications and systems such as architecture, vulnerability, methodologies, operations monitoring and data structures.

4.8.3 Document and Implement all NIST RMF controls. For DBIDS and IMESA
(PSLE CORE environment) assist with ATO accreditation documentation, Army Certificate of Net worthiness, Air Force Ability to Connect and other Service documents as determined by government approved project plan.
`

4.8.4 Support DMDC Cyber Hardening Initiative. All applications (DBIDS, IMESA) must be scanned by the specified tools (Fortify, SonaType and WebInspect), POA&M must be provided to the Cyber Hardening team for the issues identified by those tools.

4.9 Provide Security Infrastructure

4.9.1 Prepare documentation as required by NIST (Risk Management Framework) RMF to submit to the contractor that performs the Assessment and Authorization (A&A) of systems.

4.9.2 Participate in Incident response, security auditing, privacy act auditing, and monitoring of applications as directed.

4.9.3 Evaluate security technology as it applies to authentication, authorization, and auditing of in scope applications, databases and systems & provide recommendations to enhance security or comply with regulations

4.9.4 Provide Information Assurance (IA) Support; perform code reviews of developed code using code analysis tools as directed by cyber security.

4.9.5 Security Compliance & Patch Management. Cybersecurity is directed by the DMDC Cybersecurity Branch. Security compliance and patch management is a crucial element in systems administration and IT operations. IT security planning, implementation, and compliance is integral to all work performed at DMDC and, therefore, participation is a shared responsibility. The contractor is responsible for continuing to maintain security compliance support and performing patching. Patch Management is one of the major features of the enterprise suite. It encompasses researching, testing and deploying patches for remediation of vulnerabilities identified by security tools managed by the Cybersecurity Branch.

4.9.6 Perform Information Assurance Vulnerability Management (IAVM) & Situational Awareness Report (SAR) compliance patching on all servers, workstations and all other IAVM & SAR applicable assets on both the SIPRNET and NIPRNET networks. Remediation is to be completed according to IAVM or SAR guidelines as appropriate. Report IAVM or SAR patch compliance to the Cybersecurity Branch according to reporting guidelines. Deliver initial IAVM & SAR within 30 days of award; update with changes thereafter

4.9.7 All physical and logical access control IT assets must meet Security Technical Implementation Guides (STIGs) compliance prior to operating on the DMDC or Global Information Grid (GIG) network. Implement, apply and maintain STIG configuration to all IT assets. Deviations from STIG configuration setting must follow the DMDC STIG Deviation process and be approved by the Cybersecurity Branch.

4.9.8 Apply vendor supported security patches on a continuous and timely basis per DoD and DMDC policy. Patches should be applied within two weeks of release unless otherwise directed by government. Support third-party software updates and apply definitions to all applicable DMDC IT assets (e.g., network, servers and workstations).

4.9.9 All new IT assets built under this contract and baseline images must go through the DMDC Pre-production process and approved by Cybersecurity prior to operation in a production environment.

4.9.10 Install, configure, and test patches and changes required by Information Assurance Vulnerability Management (IAVM) issuances, vendor patches and STIG configuration items. Implement all necessary changes to Enterprise software and equipment in accordance with the suspense date articulated by the Cybersecurity Branch.

4.9.11 Remediate software vulnerabilities and system misconfigurations for physical and logical access control systems and applications identified in the DMDC vulnerability management tool managed by Cybersecurity Branch

4.9.12 Provide a Plan of Actions and Milestones (POAM) for remediation actions that cannot be accomplished by the Cybersecurity Branch assigned completion date.

4.9.13 Provide a STIG Deviation/Non-Compliance report for system configuration items that cannot be accomplished by the Cybersecurity Branch assigned completion date within 30 days of award and monthly thereafter.

4.9.14 Develop, implement and provide the government a Patch Management Plan that shall test and remediate vulnerabilities within the DoD timeline (currently TASKORD 13-067).

4.9.15 Correct STIG configuration items within 3 days identification by the Cybersecurity Branch.

4.9.16 Gather and collect data to support reporting of IAVM and (Federal Information Security Management Act) FISMA compliance reports and Access and Authorization (A&A).

4.9.17 Ensure all IT assets have the required cybersecurity monitoring tools (e.g., tripwire agent, HBSS agent) installed and operational in accordance with DoD and DMDC policy.
***Responsible for the up to date and compliant build, configuration and operations of the DISA provided Host Based Security System (HBSS) across all platforms associated to the OCONUS DBIDS environment and associated reporting requirements.

4.9.18 All software or hardware patches, updates, firmware must come from the DoD patch repository. Exceptions must be approved by the Cybersecurity Branch prior to engagement.

4.9.19 Provide applications services that are in compliance with and support DoD PKI or Intelligence Community (IC) policies.

4.9.20 Provide Security solutions for CE tools that meet confidentiality, data integrity, authentication, and non-repudiation requirements. Solutions shall comply with (NIST, Federal Information Processing Standards (FIPS) standards, and DoD or IC standards.

4.9.21 Coordinate patches or changes that require system or application down time with the Government and schedule during allotted maintenance hours.

4.10 Program Management

4.10.1 Provide business processes that support the integration of activities, maximizing communications among stakeholders while focusing on quality, timeliness, cost efficiency, and accuracy in the delivery of required services.

4.10.2 Business Analysis. Maintain existing government approved business requirements and add additional requirements per the scope of this PWS.

4.10.3 Identify and understand the business problem and the impact of the proposed solution on the organization's operations. Implement training methods and provide training as required.

- Provide onsite training as required for major system revisions (DBIDS 3.1 to DBIDS 5 for example)

4.10.4 Document the complex areas of project scope, objectives, and added value or benefit expectations, using an integrated set of analysis and modeling tools.

4.10.5 Evaluate customer business needs, thus contributing to strategic planning of fiscal, information systems and technology directions.

4.10.6 Work with major development and production support teams during preliminary installation and testing of new products and services.

4.10.7 Design and develop high quality business solutions; construct models, process, data, and workflow, develop business architecture: as-is and to-be models and analyze and manage requirement risk.

4.10.8 Structure requirements for traceability, prioritize requirements and draft requirement specifications.

4.10.9 Facilitate an annual Business Rules Committee and DBIDS Users Group among the appropriate stake holders as identified by the Product and Program Managers of DBIDS and IMESA. Capture and integrate all artifacts derived from the meetings.

4.11 Project Management

4.11.1 IT project managers support all phases of the software development lifecycle and shall follow the DMDC Application Development Process to manage a variety of projects, to include new development, sustainment, infrastructure projects and projects transitioning from and to DMDC infrastructure.

4.11.2 Implement a comprehensive project management approach to include technical management, schedule management, cost management, personnel management, and communication management.

4.11.3 Utilize project management best practices such as those defined in the Project Management Body of Knowledge.

4.11.4 Provide experience in multiple software development project management methodologies, to include waterfall and Scrum/Agile methodologies.

4.11.5 Allocate resource estimates to specific tasks and deliverables or sets of deliverables, including system releases.

4.11.6 Ensure all project management activities are conducted using standardized processes, to include a repeatable SDLC.

4.11.7 Provide project management support to infrastructure projects, to include system maintenance, system upgrades, migrations, and new infrastructure planning and implementation.

4.11.8 Develop project plans and follow industry standard management principles, to include risk management, critical path, resource allocation, stakeholder communication, and milestone reviews.

4.11.9 Assist in evaluating impacts to current schedules and alternative allocations of resources to minimize disruption/impacts introduced by new/changing requirements. Provide updated project schedules within 14 days of changes.

4.12 Provide Plans, Reports and Documentation

4.12.1 Provide Product Documentation and Reports

4.12.2 Senior Management Review (SMR)
The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.3 Conduct Weekly In-Progress Reviews (IPR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.4 Problem Notification Report (PNR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

4.12.5 Provide a Quality Control Plan (QCP)

4.12.6 DMDC is committed to a highly interactive relationship between quality control by the Contractor and quality assurance by the government recipient of services. This relationship shall be achieved through a Prevention Based Quality System dedicated to ensuring the best possible products and services. A copy of the comprehensive written QCP shall be submitted to the Contracting Officer (KO) and Contracting Officer's Representative (COR) within 5 working days when changes are made thereafter. The Contractor shall provide their final QCP no later than (NLT) 10 calendar days after contract award.

4.12.7 The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the contract. The Contractor's QCP shall be incorporated into and become part of this Order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the Order and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the Order.

4.12.8 RISK MANAGEMENT PLAN

4.12.9 The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this contract in a Risk Management Plan. The Risk Management Plan shall be delivered no later than (NLT) 10 calendar days after contract award.

4.12.10 WORK BREAKDOWN STRUCTURE (WBS)

Submit a final detailed Work Breakdown Structure (WBS). The WBS shall detail the decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables in accordance with the statement of work. Define each of the tasks required to complete the work, identify individual responsibilities, and describe output, timelines for completion and performance standards. The Work Breakdown Structure shall identify final completion dates and progress milestones for tasks and provides a basis for monitoring and evaluation contractor work. The WBS shall be delivered no later than (NLT) 10 calendar days after contract award.

4.12.11 Participate in Kick Off Meeting

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the contract and shall aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements at the time offers were submitted nor is it to be used to alter the final agreement arrived at in any negotiations leading to contract award. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the COR. Kick off meeting minutes shall be documented by the contractor and delivered to the Government within 3 business days of the Kick off meeting.

5 DELIVERABLES

THE CONTRACTOR SHALL SUBMIT A DRAFT VERSION OF EACH DELIVERABLE AND THE GOVERNMENT WILL PROVIDE WRITTEN ACCEPTANCE, COMMENTS AND/OR CHANGE REQUESTS, IF ANY, IN ACCORDANCE WITH PWS SECTION 5**.0. THE CONTRACTOR SHALL MAKE ANY CORRECTIONS AND SUBMIT THE FINAL DELIVERABLE, IN ACCORDANCE WITH THE DATES LISTED IN THE FOLLOWING TABLE AND IN ACCORDANCE WITH PWS SECTION** 5.0. The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) work days from Government receipt of the draft deliverable (if necessary), and sign off on the deliverable check sheet for the final draft of the deliverable within three (3) work days after the due date for submission into ITSS. After three days if not approved, the deliverable is deemed acceptable. The work products and reports shall be delivered in accordance with dates listed in the following table:

Deliverables for DBIDS/IMESA	PWS Reference	Date Due/Frequency
System design documents.	4.5.7	Architecture update prior to production release
Ad hoc Reports	4.5.11	provide status NLT 5th duty day of the preceding month
Hardware & software compatibility List	4.5.5 &4.5.6	Semi-annually
DBIDS reports (Monthly DBIDS statistics Rollup)	4.5.13	NLT 5 business day of the month
DBIDS Program Management Plan and Schedule	4.4, 4.10	Within 30 days of award; updates within 10 days of change in plans
IMESA Program Management Plan and Schedule	4.3, 4.10	Within 30 days of award; updates within 10 days of change in plans
User Training Documentation and videos of most common functions	4.5.14	update with every release thereafter
Demonstration	4.3.11.5 4.3.12.2 4.3.13.2	per Government Approved Project Plan
Training Manual/User Manual	4.1, 4.5.14	update with every release
RMF and NIST security and risk control documentation	4.8.3, 4.9.1	monthly updates and reviews
IAVM and SAR compliance Report	4.9.6, 4.9.10, 4.9.16	update with changes when appropriate
POAM	4.9.12	update with changes when appropriate
STIG Deviation/Non Compliance Report	4.5.3, 4.9.7, 4.9.13	update with changes when appropriate
Patch Management Plan	4.9.14	Critical vulnerabilities within 7 days of discovery, high

		vulnerabilities within 21 days of discovery, low vulnerabilities within 60 days of discovery.
Monthly Status Report (SMR)	4.12.2	15th of each month
QCP	4.12.5	Within 10 calendar days of award
Risk Management Plan	4.12.9	Within 10 calendar days of award
WBS	4.12.10	Within 10 calendar days of award
Kick Off Meeting Minutes	4.12.11	Within 3 business days of award
Problem Notification Reports	6.5	NLT 5 business days after identification of problem
Travel Reports	10.0	Within 5 business days of completed travel
Weekly IPR	4.12.3	Weekly

6.0 QUALITY ASSURANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

6.1 PERFORMANCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection

Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection

7.0 CONTRACTOR PERSONNEL

The contractor shall provide qualified personnel under this and ensure they possess the skills, knowledge, training required to ensure satisfactory performance of all services required.

8.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ.

9.0 CONTRACT ADMINISTRATION

9.1 Contract Type: This contract shall be firm fixed price (FFP).

9.2 Period of Performance: The period of performance (PoP) for this Task Order will be 12 months, with two optional periods of 12 months each.

9.3 Place of Performance: The work under this task will be performed on site at DMDC facilities in Seaside, CA. Any work performed at other locations shall be identified in a formal submission and approved by the Identity Division or equivalent DMDC Government division. Occasional to significant travel may also be required, as noted in PWS Section 10.0-Travel.

9.4 Hours of operation: The contractor is responsible for conducting business between the hours of 6 a.m. to 5 p.m.PT, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task will require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations (if the 24 hour support optional CLIN is exercised).

9.5 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

9.6 Telecommuting/Telework: The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of

the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following: Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.

9.7 Points of Contact:

DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. James Purdy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: James.Purdy@gsa.gov
Tel: 215-514-3952

GSA Contract Specialist (CS)
Mr. David Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contracting Officer's Representative (COR)
Mr. Shail Shah
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Shail.shah@gsa.gov
Tel: 215-446-5858

10.0 TRAVEL

It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR.
All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ

In addition, all contractor personnel under this task order shall be fully adjudicated to get a credential and some or all personnel may be required to hold at a minimum a fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. The Government may require some or all personnel under this task to hold a Top Secret with SCI security clearance.

12.0 INVOICING

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

Table of PWS Revisions

PWS Revision	Description	MOD
1	a) removed references to “draft” b) added Table of Revisions c) Revised Section 4.4.1 d) Minor edits to Section 4.2 and 4.3 e) Sections 4.5 and 4.6 revised to be Options f) Inserted New Sections 4.9 – 4.11 g) Updated Section 7 to included due dates for 4.4, 4.7, and 4.8.2 h) Updated Section 12.0 to include DMDC Point of Contact	RFQ 9/6/2019
2	a) Section 4.10 removed references to “Notifications” b) Section 15 added Appendix D and Appendix E	RFQ 9/17/2019
3	a) Section 6.0 Deliverables: update due date for Technical Roadmap, Catastrophic Cap Processes, Catastrophic Cap Recalculations Report and remove the Quality Management System deliverable	MOD 01 01/13/2020

Performance Work Statement (PWS)
Enterprise Information Technology Services (EITS) II
Defense Health Agency (DHA) Health Care Initiatives (HCI) Phase III
Task Order #47QFMA18K0030-0017
Order ID: ID03180056013

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) in support of the Office of the Under Secretary of Defense for Personnel & Readiness (OUSD P&R), Defense Human Resources Activity (DHRA) requires Information Technology (IT) services to enhance applications and products that support DMDC's Defense Eligibility and Enrollment (DEERS) applications. Support will align IT resource expenditures with business goals and objectives and enable an IT environment with innovative solutions.

2.0 BACKGROUND

The Defense Enrollment Eligibility Reporting System (DEERS) is a series of databases that come together to provide timely and accurate information on those eligible for benefits and entitlements prescribed in Department of Defense (DoD) statute, instruction, policy and regulation. It serves to prevent and detect fraud and abuse in the distribution of these benefits and entitlements and is the definitive centralized source of identity, affiliation, eligibility and enrollment verification for members of the Uniformed Services, other personnel designated by the DoD, and their eligible family members. In addition, DEERS provides statistical and demographic information to support the DoD Components and serves as the authoritative source of TRICARE benefits eligibility and the national enrollment database for TRICARE medical, dental, and special enrollments, as well as the source for fee waiver and special entitlement determinations. DMDC maintains a number of applications to support the following eligibility and enrollment core functional areas:

- Benefits Capture and Determination
- Operator and Self-Service Enrollment
- Primary Care Manager (PCM) Maintenance
- Catastrophic Cap, and Deductible (CCD)
- Fees and Premiums
- Claims Coverage
- Other Health Insurance/Standard Insurance Table (OHI/SIT)
- Person Identifier Updates
- Logon Support (i.e. DS logon, CAC)
- Customer Service
- User Access Management
- Enrollment, Management and Claims

3.0 SCOPE

The scope of this work covers the support for on-going and new development efforts, modernization of databases/data structures, data access approaches, positioning data for decision making, combining operational and reporting data, improving security and governance, and business intelligence.

4.0 PERFORMANCE REQUIREMENTS:

4.1 TASK 1 – CONDUCT PROJECT MANAGEMENT

4.1.1 Prepare and maintain a Project Management Plan (PMP) within 10 calendar days after order award. The PMP shall provide for an overall Work Breakdown Structure (WBS), risk management review; critical path; and schedule dates and dependencies. The established Project Management Plan shall be considered a living document and kept up to date and Government approved at all times. Once the project schedule has been developed and finalized, it shall be uploaded to Microsoft Project Server and published to Microsoft Project Center. Adhere to applying the Project Management Institute best practices (e.g., Project Management Body of Knowledge {PMBOK}) and DMDC Project Management Handbook (Appendix A).

4.1.2 Maintain, refine, and revise the program collaboration sites on DMDC's SharePoint site, as well as external locations when required. The contractor shall include the following documentation on the DMDC internal site: project overview documents; a consistently updated document library that preserves document history; schedules; dashboards; assignment and POC lists; summaries and agendas for all meetings and conferences attended; and support for collaborative editing/versioning of project documents.

4.1.3 Coordinate with all DMDC governance bodies is mandatory for approvals and shall be in accordance with DMDC prescribed Business Process and subsequent updates. These groups include, but not limited to, the Requirements Review Board (RRB), Architecture Review Board (ARB), Change Advisory Board (CAB), Executive Governance Council (EGC), Enterprise Quality Assurance (QA), DMDC Management Advisory Group (DMAG), Cyber Hardening Working Group (CHWG) and all impacted directorates for project requirements, dependencies and execution for approval authority. Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage.

4.2 TASK 2 - ACCELERATE FEE & PREMIUM RATE CHANGES (FEE-1)

Design and implement a fee structure that supports the rapid implementation of changes to any enrollment fee or premium rate, maintaining distinctions based on enrollment plan, beneficiary status (i.e. Group A vs Group B), and family/individual rates. Changes to fees or premiums shall be available in the environment (i.e., test or production) within five business days of receiving the new rates from DHA.

4.3 TASK 3 – CREATE A CATASTROPHIC CAP WAIVER REINSTATEMENT PROCESSES

The catastrophic cap is the most a sponsor and their family will pay out of pocket for covered health care services each calendar year. The catastrophic fee waiver indicates that no further TRICARE Prime or Select enrollment fees are due for that family for the remainder of the calendar year to which the waiver applies. Premium plans, such as Tricare Retired Reserve (TRR), Tricare Reserve Select (TRS) and Tricare Young Adult (TYA) are not affected by the catastrophic fee waiver and are not applied to the catastrophic cap. Waiver reinstatement must be in Production prior to 1 January 2020.

4.3.1 Apply all amounts reported as fee payments for TRICARE Prime and Select plans (including plus with Retired Select) to catastrophic cap computations beginning with Calendar Year (CY) 2018.

4.3.2 Reinstate the catastrophic cap fee waiver back to CY 2018, applying it to both TRICARE Prime and Select (Groups A & B).

4.3.3 Communicate add, update, or removal (inactivation) of catastrophic cap fee waiver via contractor notifications for waivers that overlap the current enrollment of a beneficiary.

4.3.4 Recalculate family catastrophic cap totals for CYs 2018 and 2019 after the catastrophic after waiver is reinstated.

4.3.5 Adjust paid through dates and store any remaining overage as a credit and Include fee and premium payments in catastrophic cap calculations.

4.3.6 Communicate changes in paid thru dates or credits via automated contractor notifications and applicable fee reports will only be done for policies that overlap the current enrollment of a beneficiary.

4.3.7 Generate a report following recalculation for CYs 2018 and 2019 that identifies the amount of overage for each retiree household that exceeded the catastrophic cap for CYs 2018 and CY 2019. Identify how it was applied (i.e. by extending the paid thru date and/or applying a credit to the policy). Coordinate with DHA.

4.3.8 Create a CCD structure that supports catastrophic cap and deductible variations based on sponsor status (Group A, Group B); differing in and out of network caps; pay plan/rank for active duty; TRR/TRS/TYA (T-Plans) vs Select vs Prime, etc. DHA will provide a chart that contains breakdown of the variations.

4.3.9 Provide a CCD structure that supports annual changes to catastrophic cap and deductible values. Changes shall be available in the specified environment (i.e. test or production) within five business days of receiving new values from DHA.

4.4 TASK 4 – CREATE AND IMPLEMENT A MEDICARE REMINDER LETTER

4.4.1 Modify letters processes to send a Medicare B Reminder Letter to beneficiaries entitled to Medicare part A at or over age 65, but not enrolled in Medicare Part B. A separate letter will be sent to beneficiaries not entitled to Medicare A at/over age 65. Letters will be a full text letter, not an email or postcard.

4.5 TASK 5 – SUPPORT THE TRICARE MEDICARE ELIGIBLE PROGRAM (TMEP) TRANSITION (OPTION)

4.5.1 Coordinate with DHA to develop detailed business requirements for program implementation and transition.

4.5.2 Support Medicare Crossover file processes:

4.5.2.1 Provide a one-time production Medicare crossover file to incoming contractor as soon as possible after security requirements and agreements are completed

4.5.2.2 Conduct weekly crossover file transmissions to incoming contractor 30 days prior to health care delivery date.

4.5.2.3 Provide file to outgoing contractor through their Period of Performance (POP) and for one week following the POP to facilitate contractor's claims processing.

4.5.3 Participate in and provide documentation for the Systems Integration Interface Meeting (SIIM) with the incoming contractor; develop presentations and facilitate discussions on the various web applications and system interfaces applicable.

4.5.4 Facilitate connectivity and connectivity testing of the various interfaces and applications.

4.5.5 Develop training materials and facilitate training for the customers including DHA and the TRICARE Contractors (may be VTC and may be face-to-face depending on the request from DHA).

4.5.6 Provide implementation support to facilitate integration testing, develop and modify test cases, compiling release notes for the external customers, facilitating the release and act as liaison between customer and DMDC Product Management.

4.6 TASK 6 – SUPPORT THE TRANSITION OF TRICARE OVERSEAS PROGRAM (TOP21) (OPTION)

4.6.1 Participate in and provide documentation for the SIIM with the incoming contractor. Develop presentations and facilitate discussions on the various web applications and system interfaces applicable to the contract/contractor.
4.6.2 Develop and facilitate the data conversion plan (includes transition from 3 to 2 overseas regions) support includes:

4.6.2.1 Update the data conversion scripts.

4.6.2.2 Execute and test the data conversion scripts and plan in all DMDC regions, coordinating with DHA and the TOP contractor on Integration Test (Contractor Test DEMO2), Stress Test, and Production regions.

4.6.2.3 Compile and transfer the enrollment Gold File.

4.6.3 Support dual operations period and contractor run-out for outgoing contractor.

4.6.4 Update the Defense Medical Information System (DMIS) table region/routing changes and/or any Service Area File (SAF) changes made by DHA as part of the contract change.

4.6.5 Facilitate connectivity and connectivity testing of the various interfaces and applications in all environments.

4.6.6 Develop material and facilitate training for the customers including DHA and the TRICARE Contractors (may be VTC or face-to-face depending on the request from DHA).

4.6.7 Provide implementation support to facilitate integration testing, developing/modifying test cases, compiling release notes for the external customers, facilitating the release and act as liaison between customer and DMDC Product Management; Support Performance Readiness Verification (PRV) and Performance Readiness Assessment and Validation (PRAV) activities.

4.6.8 Support beneficiary notification of contract transition if non-incumbent is awarded or Contractor contact information has changed.

4.7 TASK 7 - MODIFY OVERSEAS BENEFICIARY WEB ENROLLMENT (OBWE) ENHANCEMENTS FOR OVERSEAS

4.7.1 Change BWE to confirm country of residence with beneficiary (includes support for beneficiaries with non-US and APO/FPO addresses).

4.7.2 Add location and enrollment program options based on country of residence.

4.7.3 Implement the ability to update processes that account for changes to Prime and Prime Remote locations.

4.8 TASK 8 – COLLECT PERSONAL EMAIL ADDRESSES AND IMPLEMENT SECURE TEXT MESSAGING

4.8.1 Conduct analysis and provide a report that identifies use cases, requirements policies and procedures that restrict use and develop necessary changes. Include consideration of this data for surveys and educations/marketing.

4.8.2 Develop requirements and implement a system or repository to collect and authorize use of personal email addresses and text messaging for DoD purposes.

4.9 TASK 9 – SUPPORT DHA'S HIGH VALUE HEALTH PLAN MARKET DEMONSTRATION PROJECT (ACO II) (OPTION)

A TRICARE Market will be selected by DHA to test how high-value ACO's healthcare delivery model can compete for and deliver the TRICARE benefit. The market chosen for this demonstration will be heavily populated with TRICARE beneficiaries and also have a Health Plan rich environment of competing ACO organizations willing to accept risks on a capitated basis and provide the TRICARE Benefit to voluntary TRICARE enrollees. ACO II shall be in Production by October 2020 and operational January, 1 2021.

4.9.1 Support expansion of the ACO demonstrations by delivering TRICARE benefits in a second region

4.9.2 Apply fee waivers and generic Primary Care Managers to support the demonstration. Support PCM batch moves to/from ACOs as needed.

4.9.3 Develop and implement changes to self-service and operator applications to support ACO-style demonstration project requirements including zip code enforcement.

4.9.4 Develop and provide data to support beneficiary mailings; modify correspondence rules to prevent automatic beneficiary notifications.

4.9.5 Refine and expand ACO enrollment, disenrollment, and waiver reports.

4.10 TASK 10 – CREATE & MODIFY REPORTS (OPTION)

4.10.1 Modify Premium Credit report to include non-terminated policies paid out more than two years in advance with positive credits.

4.10.2 Support annual TRICARE open season reporting to DHA. Reports shall include counts for enrollments, eligible, but not enrolled, and open season usage rates.

4.11 TASK 11 – IMPLEMENT TRICARE GROUP A FEES (OPTION)

TRICARE beneficiaries Group A are sponsor's on initial enlistment or appointment occurred before January 1, 2018. Group A fee Implementation shall be in place by OCT 2020.

4.11.1 Apply Group A fees for TRICARE Select retirees and family members by effective date of January 1, 2021.

4.11.2 Terminate TRICARE Retiree Select policies/enrollments effective December 31, 2020, as directed, prior to 2021 TRICARE Open Season beginning in November 2020.

4.11.3 Support 3-5 beneficiary notifications to communicate enforcement of Select fees. Content shall come from DHA. Communication may be via mail and/or email, as specified by DHA.

4.11.4 Develop a report summarizing the number of retired beneficiaries (Group A & B) whose coverage will be terminated effective December 31, 2020. Include count of beneficiaries' eligible but not enrolled at the time of terminations. Provide output specified by DHA and generate report at the time HCDP terminations are performed (prior to open season).

4.12 TASK 12 - SURGE SUPPORT (OPTIONAL)

DMDC must respond to real-world changes, whether it is a new reform initiative, top-down policies and mandates, or even national security interests and immediate threats. It is essential that DMDC have the IT resources and means to support evolving threats. Projects include, short-term (less than 90 calendar days) response to implement directives, support to cybersecurity-related events, and surge to support complex upgrades. The contractor shall provide staffing resources within scope of the current contract to fulfill unplanned projects or unanticipated requirements. The contractor shall use industry best practices and subject matter expertise to execute additional, as needed, related projects. Surge support shall include, but is not limited to, the following activities:

- Additional resources to support the relocation of DMDC applications/systems
- Rapid capabilities that mitigate or resolve major IT issues, cybersecurity threats, national security events, policy changes, and impacts
- Implementation of new DHA programs
- Transition or transfer of existing DoD programs

The contractor shall account for additional as-needed activities and provide the resources necessary to accommodate them. During the life of this contract the workload in any one area may grow significantly for a period of time. When a surge requirement is identified by the Government, the surge CLIN will be exercised. The Contracting Officer or Contracting Officer's Representative (COR) will provide the contractor with a requirements document specifying the

surge requirement, and expected outcomes. The contractor shall develop a Surge Plan which shall include, project approach, milestones and schedules, and detailed resource information to be reviewed and approved by the Government. The contractor shall staff surge resources within 30 calendar days of formal written approval of the Surge Plan. The Government shall use existing performance metrics and SLAs to measure surge-related performance.

5.0 SUBMIT REPORTS & DOCUMENTATION

5.1 Technical Roadmap

The Contractor shall follow the Technical Roadmap requirements identified in the PWS Section 5.8.1 of the EITS II Base IDIQ.

5.2 Risk Management Plan

The Contractor shall follow the Risk Management Plan requirements identified in the PWS Section 5.8.3 of the EITS II Base IDIQ.

5.3 Meeting Summaries

The Contractor shall follow the Meeting Summaries requirements identified in the PWS Section 5.8.4 of the EITS II Base IDIQ.

5.4 Weekly In-Progress Review (IPR)

The Contractor shall follow the IPR requirements identified in the PWS Section 5.8.5 of the EITS II Base IDIQ.

5.5 Monthly Status Report (MSR) and Senior Management Reviews (SMR)

The Contractor shall follow the MSR and SMR requirements identified in the PWS Section 5.8.6 of the EITS II Base IDIQ.

5.6 Problem Notification Report (PNR)

The Contractor shall follow the PNR requirements identified in the PWS Section 5.8.7 of the EITS II Base IDIQ.

5.7 Contract Discrepancy Report (CDR)

The Contractor shall follow the CDR requirements identified in the PWS Section 5.8.8 of the EITS II Base IDIQ.

5.8 Semi-Annual Subcontract Report

The Contractor shall follow the Semi-Annual Subcontract Report requirements identified in the PWS Section 5.8.9 of the EITS II Base IDIQ.

5.9 Quality Management System

The Contractor shall follow the Quality Management System requirements identified in the PWS Section 5.9 of the EITS II Base IDIQ.

5.10 Quality Control Plan (QCP)

The Contractor shall follow the QCP requirements identified in the PWS Section 5.9.1 of the EITS II Base IDIQ.

5.11 Quality Assurance

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.9.2 of the EITS II Base IDIQ.

6.0 DELIVERABLES

All deliverables and work products shall be submitted to the COR in electronic format for acceptance and approval. The acceptance of deliverables and satisfactory work performance shall be based on the timeliness, accuracy and standards as specified in the requirements of the PWS.

PWS Section	PWS Section	Date Due/Frequency
4.1.1	Project Management Plan(PMP)	Draft due within 10 days of order award Final due in accordance with Inspection and Acceptance clause Updated as changes take place
4.1.2	Maintain SharePoint sites	Updated 10 days after award and updated within 2 days after documents change
4.2	Accelerate Fee & Premium Rate Changes	In production by November 1, 2019
4.3	Update Catastrophic Cap Processes	~~In production by January 2020~~ In production by June 20, 2020
4.3.7	Catastrophic Cap Recalculations Report	~~In production by June 1, 2020~~ In production by June 20, 2020

4.4	Medicare Reminder Letter	Completed by end of Q2 of Base Period
4.5.2.1	TMEP Crossover File (Incoming)	Per Government approved Project Management Plan
4.5.2.3	TMEP Crossover File (Outgoing)	Per Government approved Project Management Plan
4.5.4	Establish TMEP Connectivity & connectivity testing	Per Government approved Project Management Plan
4.5.5	TMEP Training & Training Documentation	Per Government approved Project Management Plan
4.6.2	TOP21 Data Conversion Plan	Per Government approved Project Management Plan
4.6.4	Defense Medical Information System (DMIS) table update	Per Government approved Project Management Plan
4.6.5	Establish TOP21 Connectivity & Connectivity Testing	Per Government approved Project Management Plan
4.6.6	TOP21 Training & Training Documentation	Per Government approved Project Management Plan
4.6.7	TOP21 Implementation Support	Per Government approved Project Management Plan
4.7	Overseas BWE Changes	Completed by end of Q3 of Base Period
4.8.1	Email & Text Message Analysis	60 Days after award

4.8.2	Personal Email & Text Message Implementation	Completed by 30 prior end of contract expiration
5.1	Technical Roadmap	~~30 days after contract award~~ 60 calendar days after contract award and 45 calendar days after each option year is exercised
5.2	Risk Management Plan	30 days after award, update as needed
5.3	Meeting Summaries	1 day after the meeting
5.4	Weekly IPR	Weekly - Written report is due 1 day prior to meeting
5.5	Monthly MSR	MSR shall be conducted on the 15th working day of each month; electronic copy of brief shall be delivered 3 days prior to the brief.
5.6	Problem Notification Report	3 days after identification of problem
5.7	Contract Discrepancy Report	Respond to CDR in accordance with the requests from GSA Contracting Officer
5.8	Semi-Annual Subcontract Reporting	The report shall be submitted after each 180 days of performance
~~5.9~~	~~Quality Management System~~	~~15 days after contract award, update as needed~~
5.10	Quality Control Plan	15 days after contract award, update as needed
5.11	Quality Assurance Plan	15 days after contract award, update as needed

12.4	Post Award Conference	Within 5 days of award

7.0 Performance Standards

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

Performance Standard	**Acceptable Quality Level (AQL)**	**Method of Surveillance**
Functionality of the software to meet required systems architecture and processing capabilities	Functionality defined in the requirements must be prioritized and tolerances for deviation assigned for each component. AQL: 95% of operational capability.	Independent verification & validation (IV&V) for testing new releases of software to determine that previous functionality is maintained. Customer satisfaction as measured through validated customer complaints, feedback, and surveys. For conversion projects, independent verification & validation (IV&V) for developing or maintaining system processing/benchmark during parallel processing.
Delivery dates are met	95% compliance	100% inspection

Meet all Government and agency specific requirements	Draft outputs to meet 90% compliance; and revised final outputs to meet 100% compliance	100% inspection to ensure that all Government and Agency specific requirements have been met. Independent verification of security procedures-defined by agency (could be performed by a third party or another agency according to current security regulations and measures**.**
Software adds value and improves existing functionality without negatively impacting the existing operational environment.	Base line functionality is met at 90% at initial testing with production meeting 100%. Non critical functionality is met at 80%	Independent Verification and Validation (IV&V) for testing new releases of software to determine that previous functionality is improved. Customer satisfaction is measured through validated customer complaints and surveys.
Project Management Plan	90% of areas required by government including the WBS are created and updated monthly with draft; 100% with Final. 95% On time delivery of Initial and Monthly Updates	100% Inspection
Quality Control Plan	95% On time delivery of Initial and Monthly Updates	Random Monitoring and Partial Inspection Quarterly by COR
Risk Management Plan (RMP) RMP delivered on-time and updated monthly	95% on time delivery of initial RMP with no more than five (5) errors 95% delivery of updates by last workday of each month.	Routine inspection of deliverable products and services.
Release and Production Drop Schedules	Schedules consistently depict well-planned, staged and sequenced activities. Schedules make optimal use of the resources.	Schedules reviewed at the Weekly IPR Explanation of scheduled and unscheduled changes shall be provided during regularly

	Flexibility and decision-making shows a consistent ability to promptly identify, evaluate, react and incorporate, into planning and implementation issues as they relate to meeting release and production schedules.	scheduled IPR Observation of Key Government POCs
Customer Satisfaction	Provides value-added advice/thought leadership and deliverables that reflect the DMDC's needs to achieve program success. 95% satisfaction	Help desk surveys, Annual Past Performance Evaluation
Responsiveness	Responds to staff and acknowledges inquiry within one business day 95% response to all inquiries	Direct Observation
Communications (Oral and Written)	- Quality: Provided information that was accurate in technical content, transparent, clear, and relevant. - Timely: Presented information in a timely manner which kept the Government informed of the status on assigned tasks, action items, projects, and service delivery issues. - Pro-active: Engaged in proactive communications regarding project status, scheduling, cost control, pending staffing changes, and actions taken to resolve problems. AQL: Communications enable Task Order requirements to be met on time.	Observation Random Inspection

Effective Contractor To Government Partnership	Demonstrated initiative and foresight to identify novel solutions, or offer innovative insights. Melds best-of-breed approaches and industry best practices to address agency challenges. - Champions process improvements or enhancements that result in the compression of timelines, efficiencies in operations, or savings AQL: Positive work relationship with Government POCs.	Observation Stakeholder Feedback

8.0 Non-Disclosure Requirements

The Contractor shall follow the Non-Disclosure requirements identified in PWS Section 8.6 of the EITS II Base IDIQ.

9.0 Cooperation with Other On-Site Contractors

The Contractor shall follow the Cooperation with Other On-Site Contractors requirements identified in PWS Section 11.7 of the EITS Base IDIQ.

10.0 Quality Surveillance

The Government may follow the Appendix P - Quality Assurance Surveillance Plan to EITS II IDIQ Base Contract

11.0 Contractor Administration

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

11.1 Contract Type

Firm Fixed Price

11.2 Period of Performance

The period of performance for this Task Order shall be 12 months from date of award.

11.3 Place of Performance/Hours of Operation

At least 50% of the work under this task shall be performed on site at DMDC facilities in Seaside, CA. The remaining work can be performed at a contractor provided facility. Any work performed at other locations shall be identified in the contractor's formal submission and approved by the Government.

12.0 Government Points of Contact

GSA Contracting Officer (CO)
Mr. Alexander Garcia
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: alexander.garcia@gsa.gov
Tel: 215-446-5868

GSA Contracts Specialist (CS)
Michael Levy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: michael.levy@gsa.gov
Tel: 215-446-5806

GSA Project Manager / Contracting Officer's Representative (COR)
Mr. Wesley Mellon
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor, 100 S. Independence Mall West, Philadelphia, PA 19106
E-mail: Wesley.Mellon@gsa.gov
Tel: 215-446-4566

Alternate GSA Project Manager / COR
Ms. Carol Carpenter
E-mail: Carol.Carpenter@gsa.gov
Tel: 301-737-2493

DMDC Points of Contact (POC)
Pamela Bridges
Defense Manpower Data Center
E-mail: pamela.r.bridges.civ@mail.mil
Tel: (831) 583-4044

12.1 Government Furnished Property/Equipment/Information (GFP/GFE/GFI):

The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ.

12.2 Travel:

Local or long-distance travel may be required to various locations CONUS. The annual travel estimate is $0. The Contractor shall follow the travel requirements identified in Section 10.7 of the EITS II PWS.

12.3 Security:

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

12.4 Post Award Conference:

The Contractor shall follow the Post Award Conference requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

13.0 Inspection, Acceptance, and Payment:

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

14.0 Invoicing:

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

15.0 Appendices:

Appendix A – Project Management Process Handbook
Appendix B - Implementation of Group A Fees
Appendix C - Functional Requirements Matrix
Appendix D - Medicare Part A and B Reminder Letter
Appendix E - Medicare Part B Reminder Letter

Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services (EITS)
Task Order ID – ID03180056010
Secure Internet Protocol Router (SIPR) Token Support

1.0 INTRODUCTION

Defense Manpower Data Center (DMDC) requires Secure Internet Protocol Router Network (SIPRNet) token support for the exchange of Extensible Markup Language (XML) files and the extraction of card inventory forecast data from the Public Key Infrastructure (PKI) Token Management System (TMS) to support cardstock order/invoice activities.

2.0 BACKGROUND

In 2011, the Director, Operational Test and Evaluation (DOT&E) identified the need for a centralized method to track shipments of SIPRNet tokens from the manufacturer to the System Administrators, and provide management of the lifecycle of the token from manufacture to termination. The Department of Defense (DoD) Public Key Infrastructure (PKI) Program Management Office (PMO) decided to leverage the DMDC Inventory Logistics System (ILS), which manages the logistics for the Common Access Card (CAC) on the Non-Classified Internet Protocol Router Network (NIPRNet). An additional instantiation of the CAC-ILS was deployed for the management of the SIPRNet token in May 2012, called SIPR-ILS. In May 2017 the TMS Central Management of Tokens (CMT) functionality took over the logistics functionality from the SIPR-ILS. DMDC continues to facilitate the exchange of .XML files between the TMS and Smart Card manufacturers.

3.0 SCOPE

The contractor shall provide the personnel and management necessary to support the current SIPRNet Inventory Token support activities.

4.0 REQUIREMENTS The Contractor shall:

4.1 REQUIREMENTS FOR MANAGING CARD PRODUCTS

Support the exchange of the XML descriptor file parameters and descriptions with TMS and card suppliers for incorporation into the TMS inventory management system in accordance with the latest version of the Pre-Issuance Technical Requirements (PITR).

4.2 SIPR Token Requirements for Order Communications:

4.2.1 Conduct joint testing with the PKI PMO for files coming from TMS to the manufacturers (e.g., changes in xml file schema; refresh of PKI signing/encryption keys). Support will be on an as needed basis during times of testing. DMDC anticipates two annual test events requiring 10 hours of testing each.

4.2.2 Employ the operational Secure File Transfer Program (SFTP) receiving site where PKI PMO

securely uploads the XML descriptor files (i.e., Batch Order Descriptor (BOD)/ Shipping Order Descriptor (SOD)) that communicate the production order data.

4.2.3 Perform BOD/ Batch Delivery Descriptor (BDD) and SOD/ Shipping Delivery Descriptor (SDD) processing to support SIPR Token-related activities. This includes troubleshooting procedures for card vendor file exchange issues; and support for signed and encrypted card product file exchange with SafeNet.

4.2.4 Employ the XML Transfer Tool to sign and encrypt and decrypt and remove a signature from XML files exchanged between TMS and the cardstock manufacturers.

4.2.5 Leverage the token test lab to put certificates on test tokens. This task does not include the cost of the test tokens.

4.3 REQUIREMENTS FOR SIPR TOKEN PROGRAM MANAGEMENT SUPPORT:

4.3.1 Support issue resolution about shipments and tokens from token program managers from the Military Services and DoD agencies. These may include tracking down lost/missing shipments, generation of replacement card orders, researching token arrivals from the manufacturer, etc. Currently there are less than twenty token program managers.

4.3.2 Coordinate with the Defense Information Systems Agency (DISA) to keep them informed of changes in card products that impact middleware vendors, data model changes, architecture changes, and any change that will/could impact card issuance on the Token Management System.

4.3.3 Support the continued development and maintenance of the token roadmap.

4.4 SUBMIT REPORTS

4.4.1 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.9.6 of the EITS II Base IDIQ.

4.4.2 Participate In Kick-Off Meeting

This meeting shall provide an introduction between the Contractor personnel and Government personnel who will be involved with the contract. The meeting shall provide the opportunity to discuss technical, management and security issues. The Kick-Off Meeting will aid both the Government and Contractor in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable. The Contractor shall provide a written summary of the Kick-Off Meeting the DMDC PM and GSA COR.

4.4.3 Problem Notification Report (PNR)

The Contractor shall follow the PNR requirements identified in PWS Section 5.9.7 of the EITS II Base IDIQ.

5.0 DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within ten

(10) work days from Government receipt of the draft deliverable. The work products and reports shall be delivered in accordance with dates listed in the following table

Deliverable	PWS Ref.	Delivery Date
Joint Test & Summary with the TMS and the DISA Team	4.2.1	As needed and requested by the Government
Senior Management Review (SMR)	4.4.1	No later than the 15th of each month
Problem Notification Report	4.4.3	Within 3 working days of identification of problem.
Kick-Off Meeting	4.4.2	Within 10 working days of TO Award
Written Summary of Kick-Off meeting	4.4.2	Within 10 working days of TO award

5.0 SECURITY

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ. In addition, all contractor personnel under this task order shall hold fully-adjudicated and active Public Trust clearances. Contractor personnel shall possess these security clearances at Task Order award.

The Government requires the contractor to establish that applicants or incumbents either employed by the Government or working for the Government under this contract are suitable for the job and are eligible for a public trust position at the appropriate level ***prior to contract award*** date. This includes the following:

- US Citizen
- Favorable FBI fingerprint check
- Fully adjudicated background investigation completed

6.0 QUALITY SURVEILLANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.11 of the EITS II Base IDIQ.

6.1 Contract Discrepancy Report (CDR)

The Contractor shall follow the requirements identified in PWS Section 5.9.8 of the EITS II Base IDIQ.

6.2 Performance Objective and Thresholds:

The table below identifies the Critical Performance Elements and the respective Performance Standards and Acceptable Quality Levels (AQLs) which the Government will use to determine contractor

performance. The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation. Failure to meet the performance metrics below will result in negative past performance evaluations.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	Method of Surveillance
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection

6.3 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

• Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.

• Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.

• Specifications Validity – All Deliverables must satisfy the requirements of the Government.

• File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.

• Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.

• Timeliness – Deliverables shall be submitted on or before the due date specified.

7.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

The Government will provide access to: the DMDC landing site for the XML file exchange; a SIPRNet Terminal for accessing the TMS; and those servers and applications required to perform the requirements of this PWS. . No other GFE is anticipated.

8.0 APPLICABLE DOCUMENTS

Document	Web link
DoDI 8500.01, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

9.0 PLACE OF PERFORMANCE

The majority of work performed will be at the Government's facility at the Mark Center in Alexandria, VA. At the Government's direction, the contractor shall attend meetings within the National Capitol area, to include but not limited to the Pentagon, the Hoffman Building, Tysons Corner and Herndon, VA. Occasional travel may also be required, as noted in PWS Section 10.0- Travel.

9.1 PERIOD OF PERFORMANCE

The period of performance for this task order shall be 12 months from date of award with two (2) 12-month option periods.

10.0 TRAVEL

The cost reimbursable not-to-exceed travel limit is estimated at $5,000.00 for each period of performance. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. Before contractor travel is executed, authorization must be given by the DMDC COR and GSA COR.

All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 INSPECTION, ACCEPTANCE AND PAYMENT

11.1 The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

11.1.1 Delivery Address

All deliverables shall be submitted to the designated DMDC POC's. Additionally, if directed, the Contractor shall upload the deliverables into the GSA ITSS Portal.

11.1.2 Method of Delivery

The Contractor shall provide all deliverables and reports in the format of which to be defined or approved by the Government and subject to change over the course of the task order.

11.1.3 Acceptance Criteria

Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in EITS II Contract ID03180056 and all terms and conditions of this Task Order, including all modifications.

11.1.4 Acceptance of Deliverables

The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 days, the Contractor shall not assume that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 working days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

11.2 Invoicing

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Non-secure Internet Protocol Router Network (NIPRNet)
Enterprise Alternate Token System (NEATS) IV

1.0 INTRODUCTION

The Department of Defense (DOD) Public Key Infrastructure (PKI) Program Management Office (PMO), through the Defense Manpower Data Center (DMDC), requires information technology services that can support the development, sustainment and delivery of a DOD PKI certificate and token issuance system for NIPRNet. Its primary purpose is to serve people who require alternate tokens that are not Common Access Cards (CACs) to access NIPRNet information systems and email services.

2.0 BACKGROUND

2.1 DMDC supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's, covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data on the Uniformed Services. These data support decision-making by the Office of the Secretary of Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD.

2.2 DMDC operates major programs that include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD pay and benefit systems; personnel and property identification, authentication, and access control systems; personnel evacuation support systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and post-service job searches. DMDC is a geographically separated organization with personnel and facilities located in both Virginia (VA) and California (CA) and support offices in Germany, the Republic of Korea, Qatar and Kuwait. The Director of DMDC is located at DMDC's offices in Alexandria, VA.

2.3 The major components of DMDC's information technology (IT) environment, major programs and customer off the shelf (COTS) software supported by this PWS are described in Appendices A through J. DMDC anticipates that these components, applications and information may change before and during the performance of this effort.

3.0 SCOPE

The Contractor shall provide the personnel and management required to support in planning, designing, developing, updating, sustaining and Quality Assurance for the NEATS system for the Department of Defense.

All application development and other DMDC support must comply with the current approved, DMDC enterprise reference architecture(s), policies, and procedures identified by the Government and documented in alignment with the Department of Defense Architecture Framework (DoDAF) (Appendix K).

4.0 REQUIREMENTS. *The contractor shall:*

4.1 Provide Sustainment Support for the NEATS and Alternate Token Issuance Management System (ATIMS) Applications

4.1.1 Provide software development and sustainment as NEATS and ATIMS solutions are fielded into production.

4.1.1.1 In conjunction with the ATIMS Program Manager (PM), maintain the ATIMS baseline, and execute only DMDC-ATIMS Configuration Control Board (CCB) approved modifications.

4.1.1.2 Modify fielded software to identify new requirements, change existing requirements, develop, test, and field routine software changes. CCB-approved code changes are to be developed according to DMDC standards, and these changes must be documented in release notes according to DMDC standards to reflect the functional changes. Release notes shall be written within 3 calendar days of a release implementation.

4.1.1.3 The contractor shall maintain the ATIMS user guide at Https://intelshare.intelink.gov/sites/neats/_layouts/15/start.aspx#/ . The contractor shall keep it current with ATIMS ensuring all functionality changes to ATIMS application are reflected in the user guide. Updates must be available to the ATIMS PM after Quality Assurance (QA) approval but before the scheduled production release.

4.1.1.4 Provide application sustainment which includes: processes, procedures, people, material, and information required to support, maintain, and operate the software aspects of a system.

4.1.1.5 Ensuring application sustainment includes: architecture, technical currency, DoD instruction or policy directives, legislative directives, engineering, data management, configuration management, training, survivability, environment, and protection of critical program information, anti-tamper provisions, information technology security, supportability and interoperability functions, product management, and technology refresh.

4.1.1.6 Evaluate release scope for all releases for production planning. Release scope detail shall be posted within the current DMDC release tool (JIRA).

4.1.1.7 Provide monthly updates to the Government on the application sustainment.

4.1.1.8 The government anticipates 3 releases per year incorporating required updates for cybersecurity and necessary engineering change proposals (ECPs).

Release Type	Est Hours to complete	QTY per year
Cyber/ECP/QA	960 per release	3

4.1.1.9 Tier 2 Help Desk support
Monitor and respond to Tier 2 tickets supporting customer product installation and trouble shooting. There will be an average of 100 tickets per month with an estimated time of 2 hours to resolve each.

Ticket Action	Timeframe
Triaged/assigned (100%)	Within 2 Business Days
Resolved (90%)	Within 10 Business Days
Escalated	If ticket cannot be resolved within 10 business days, it will be escalated to government lead for awareness.

4.2 Provide Quality Assurance (QA) Support

4.2.1 Provide NEATS and ATIMS Quality Assurance Testing and Quality Management Planning in accordance with the processes and procedures established in the base PWS for EITS II and EITS TO 2. Define and develop test plans, test scripts, test cases; track and report issues; conduct testing and measure the success during and after testing; and evaluate and document test results. Conduct Quality Assurance (QA) for DMDC projects, using documented requirements provided in functional, technical or application release scope specifications. Provide QA support, which includes releases for: Shared libraries, single table updates, web applications, web services, applications, reports, modules, software programs, etc.

4.2.2 The QA specific performance objectives are within scope. Maintain the automated and manual test case reports metric for the transitioned applications during the remaining period of performance. Report current state (automated and manual metrics) for the period of performance. Deliver a current and future state assessment of incorporating automation within the applications in scope, before the end of the current period of performance.

4.2.3 **Provide Quality Assurance Test Strategy Support**

4.2.3.1 Develop QA Testing Strategy which outlines the QA process that will be used to validate all tested items perform as designed, fulfill requirements, meet any applicable service level agreements and does not adversely impact other applications.

4.2.3.2 Ensure the Quality Assurance Test Strategy defines a clear and consistent strategy that supports the following areas:

- Validation of Software Readiness for QA Testing
  - (Release Notes, Developer Handoff)
- Creation and maintenance of RTMs
- QA test case suites for automated and manual testing
- Automation scripting
- Issue tracking and issue resolution
- Test data creation and management
- QA testing sign off process
- QA requests for approval in support of software deployments as applicable.

4.2.3.2.1 Incorporate the Quality Assurance Test Strategy consistent with existing DMDC QA standards, guidelines, and document templates. DMDC QA standards, guidelines and document templates will be provided upon award.

4.2.4 **Quality Assurance Test Plans**

4.2.4.1 Create and submit for approval the QA Test Plans which provide a detailed listing of all QA activities within each QA testing project. QA Test Plans must be developed and maintained for all projects requiring QA level support.

4.2.4.2 QA test plans must accommodate regression testing of software components and functionality that has not been modified but may interact with modified components and functionality to ensure that changes have not adversely affected existing capabilities.

4.2.4.3 QA test plans must include coverage for Section 508 Accessibility validation, based on direction from the QA government lead, regarding level of test coverage, and targeted applications within scope.

4.2.4.4 QA test plans must specify the software and versions under which the application was tested. If different from previous QA test, this information must be updated in the ATIMS Workstation Setup Guide found at https://intelshare.intelink.gov/sites/neats/_layouts/15/start.aspx#/.

4.2.5 Release Deployment Monitoring

4.2.5.1 Provide support during deployment of releases

4.2.5.1.1 After hour support is anticipated to ensure no issues are encountered when releases are placed into production

4.2.5.2 Submit report to the Government PM and the COR within 72 hours of a release deployment. At a minimum the report shall have: who deployed release, status of release after deployment and any actions necessary based on data from release.

4.2.5.2.1 Five business days after release, report shall be updated to reflect any issues or concerns and carry overs to the next release. At a minimum, all work arounds shall be documented and approved by the Government PM.

4.3 Reports

4.3.1 Provide a Quality Control Plan (QCP)

The Contractor shall follow the QCP requirements identified in the PWS Section 5.9.1 of the EITS II Base IDIQ

4.3.2 RISK MANAGEMENT PLAN

4.3.2.1 The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this contract in a Risk Management Plan, which shall be submitted to the Government 30 calendar days after Task Order Award. Escalate issues and risks within 24 hours of identification to the Government PM and COR via e-mail.

4.3.3 Work Breakdown Structure (WBS)

4.3.3.1. Submit a final detailed Work Breakdown Structure (WBS) 30 calendar days after Task Order Award. The WBS shall detail the decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables in accordance with the PWS. Define each of the tasks required to complete the work, identify individual responsibilities, and describe output, timelines for completion and performance standards. The WBS shall identify final completion dates and progress milestones for tasks and provide a basis for monitoring and evaluation of contractor work.

4.3.3.2 The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the requirements of the PWS. The Contractor's QCP shall be incorporated into and become part of this task order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the contract and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the contract.

4.3.4 Participate in Kick Off Meeting

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the contract and will aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements at the time offers were submitted nor is it to be used to alter the final agreement arrived at in any negotiations leading to contract award. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the DMDC PM and GSA COR.

4.3.5 Weekly Status Meeting

Facilitate weekly status update meetings providing a review of project schedule, issues and risks. Distribute the prior week's meeting minutes at least 2 business days prior to the next meeting. Update project schedule on a real-time basis as events require, and publish to the Project Center immediately after updates are made. Maintain the project notebook, which is currently maintained in OneNote, and maintain in accordance with the meeting minutes' content.

4.3.6 Monthly Status Report (MSR) and Senior Management Reviews (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.3.7 Problem Notification Report (PNR)

The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ.

5.0 Quality Surveillance

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

5.1 Performance Standards:

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative

assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

Performance Objective	Performance Threshold	Method Of Surveillance
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) business day of the negotiated suspense.	Contractor shall submit to the product owner for review and approval. The product owner shall maintain a log on submitted deliverables and corrections required and submit to the COR monthly.
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) business days.	The log will identify the timetable and schedule for on time submission
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) business day of initial government notification.	Product Owner will log government requests for solutions on the log
QA Specific Objectives	Provide the percentage of test case execution. Unless otherwise agreed upon with the government project manager, test case execution must be 100% for all projects. Provide on the signoff documentation to project teams. % of test case execution (indicates the progress of testing by giving the percentage of test cases executed with the result of a pass, fail, or blocked result) Percent of Test Case Execution = (Number of Passed Tests + Number of Failed Tests + Number of Blocked Tests) / Number of Test Cases	Product Owner will track and manage QA releases twice a year and log all actions.

	Provide the defect removal efficiency. DRE must remain >95%. Report progress in MSR. Defect Removal Efficiency (No. of Defects found during QA testing / (No. of Defects found during QA testing +No. of Defects found by End user))	
	Provide defect leakage rate. Rate must remain at 5% or less. Report progress in MSR. Defect Leakage (used to identify the efficiency of the QA testing) = (No. of Defects found in UAT / No. of Defects found in QA testing) * 100	
	Automation shall meet requirements established in TO 2 Enterprise QA.	
	Continue ongoing monitoring of PII data and its usage.	
	4.8.3.1 Respond to all calls related to incidents affecting production within fifteen minutes, in the event that the incident requires QA to test a behavior in production. Report progress in MSR.	

5.8 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.

- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

5.9 The Government will provide written acceptance, comments and/or change requests, if any, within 5 business days from Government receipt of the draft deliverable.

Deliverable	**PWS Section**	**Due Date**
PWS Section 4.1 NEATS & ATIMS Sustainment		
Software Release Notes	4.1.1.2	At least 3 calendar days prior to production release.
Updates to User Guides and Manuals	4.1.1.3	After QA release approval but prior to production release.
Monthly Status Report	4.1.1.7	Monthly
PWS Section 4.2 Quality Assurance		
Quality Management Plan	4.2.1	Updated upon request by government.
QA Metrics	4.2.2	Within 7 calendar days of QA support begin date, or upon request by government.
QA SharePoint site maintenance	4.2.1	Weekly or upon request by government.
QA Testing Strategy	4.2.3	Updated upon request by government.
Staffing Plan	4.2.1	Within 10 calendar days of award.

Automated Test Scripts	4.2.1	Within 7 calendar days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Manual Test Case Report	4.2.2	Monthly with MSR reporting
Automated Test Case Report	4.2.2	Monthly with MSR reporting.
QA Test Plans	4.2.4	Within 7 calendar days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Level of Effort and Resource Estimate	4.2.1	Initial estimate provided within 2 business days of project notification; final provided within 7 calendar days of project finalization notification.
Requirements Traceability Matrix (RTM)	4.2.3	Updated within 7 calendar days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Testing Results and Change Management System (CMS) Region level readiness	4.2.1	7 calendar days prior to release to planned production or contractor test environment.
Issue Tracking Tickets and Reporting	4.2.1	Issues logged within 24 hours of discovery and reports

508 Compliance Audit Report	4.2.4	Quarterly; provide report within 7 calendar days of concluded audit.
Deployment monitoring Report	4.2.5	Submit report to Gov PM and COR within 72 hours of deployment
QA In Progress Review (IPR) Agenda	4.2.1	Weekly.
QA IPR Meeting Minutes	4.2.1	Within 48 hours of IPR meeting
QA Off Hours Reporting	4.2.1	Weekly
Functional and Technical Meetings	4.2.1	Weekly/Monthly/Ad Hoc.
PWS Section 4.3 Reports		
Risk and Issue Identification	4.3.2.1	Within 24 hours of notification
Work Breakdown Structure	4.3.3.1	30 calendar days after TO Award
Project Schedule	4.3.5	As events dictate changes (close to real-time)
Project Notebook	4.3.5	Weekly
Meeting Minutes	4.3.5	Weekly, within 2 business days prior to next weekly meeting

6.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the Contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets, copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

The Government will provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; commercial off-the-shelf software; hosting facilities; and all other relevant materials and

equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support.

7.0 PLACE OF PERFORMANCE / HOURS OF OPERATION

7.1 The work under this task will be performed off site.

7.2 The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 2 support, production implementations and release deployment monitoring and remediation as needed.

7.3 The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following:

- Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.

- Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment

8.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order will be 12-months from date of award (with two (2) 12 month option periods).

9.0 CONTRACTOR TRAVEL

9.1 The Government does not anticipate any travel. However, should travel be required, the following applies.

9.2 Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. Before contractor travel is executed, authorization must be given by the COR.

9.3 All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

9.4 Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

9.5 Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

10.0 SECURITY

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ. In addition, all contractor personnel under this task order shall hold fully-adjudicated and active Public Trust clearances. Contractor personnel shall possess these security clearances at Task Order award.

The Government requires the contractor to establish that applicants or incumbents either employed by the Government or working for the Government under this contract are suitable for the job and are eligible for a public trust position at the appropriate level ***prior to contract award*** date. This includes the following:

- US Citizen
- Favorable FBI fingerprint check
- Fully adjudicated background investigation completed

11.0 INSPECTION, ACCEPTANCE AND PAYMENT

11.1 The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are

responsible for inspection and acceptance of all services, incoming shipments, documents and services.

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

11.6 Invoicing

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

1.0 APPENDICES

Appendix A – Software Development Roadmap

Appendix B – Automation Standard Best Practices

Appendix C – Enterprise QA Roles and Responsibilities

Appendix D – DMDC ARB Charter References (Enclosure 1)

Appendix E – DMDC ARB Charter Required Artifacts (Enclosure 2)

Appendix F – DMDC ARB Charter Process Map and Description (Enclosure 3)

Appendix G – DMDC ARB Charter

Appendix H – CEAS Project Charter

Appendix I – CEAS Reports List

Appendix J – Template Checklist

Appendix O – EHRM Applications

12.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

Table of PWS Revisions

Rev. No.	C.1.1.1 Rev. Date	**Name**	C.1.1.2 Description	**TO Mod No.**
1	8/13/19	SO	Added Section Task 12 (Support Accountable Care Organization (ACO) Demonstration), Add the ACO Deliverables to Section 6.7, and corrected the Performance Threshold for the Application & System Security Compliance in the under Section 7 Performance Standards.	3

Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
Software Development Maintenance Services (SDMS)
Order ID: 47QFMA18K0030-0001/ID03180056006

1.0 INTRODUCTION

The Defense Manpower Data Center requires Software Development Maintenance Services (SDMS) to support the sustainment and maintenance of existing software applications, legacy systems, databases and interfaces.

2.0 BACKGROUND

Software sustainment is growing in importance as the inventory of DoD systems continues to age and greater emphasis is placed on efficiency and productivity in defense spending. A key mission for the DMDC is the development and maintenance of it applications, systems, databases and interfaces. Systems are increasingly reliant on software which must be sustained into the future. To sustain these systems organizations must define sustainment meet criteria to enter sustainment and overcome sustainment challenges.

While DoD Instruction 5000.02 describes sustainment in detail the Institute of Electrical and Electronics Engineers (IEEE) Standard Glossary of Software Engineering Terminology defines "software maintenance" as the process of modifying a software system after delivery to correct faults, improve performance or adapt it to a changed environment. It involves orchestrating the processes, practices, technical resources, information, and workforce competencies for systems and software engineering, to enable systems to continue mission operations and also to be enhanced to meet evolving threat and capability needs.

Sustaining software for the DoD, however, requires attention to certain issues (such as operations and training) that are less essential in commercial software maintenance. There are four primary categories of software sustainment activities:

- Corrective sustainment diagnoses and corrects software errors after release
- Perfective sustainment upgrades existing software to support new capabilities and functionality
- Adaptive sustainment modifies software to interface with changing environments
- Preventive sustainment modifies software to improve future maintainability or reliability

3.0 SCOPE

The scope of this work covers the full range of development and maintenance IT services to ensure uninterrupted service of existing applications, systems and related software; capturing user requirements; database administration; identifying functional, security, and performance requirements; providing design and program documentation, and supporting the Risk Management Framework (RMF) process.

4.0 OBJECTIVE

The objective of this task order is to identify and implement best commercial practices to modernize, streamline, centralize and standardize software development and sustainment in a more evolvable architecture that can better leverage state of the art computing capabilities in order to deliver the best available technology, reduce program sustainment costs, and maximize system reliability and performance.

5.0 PERFORMANCE REQUIREMENTS

The Contractor shall provide support for the tasks described below:

5.1 TASK 1 – PLANNING & MANAGEMENT OF SOFTWARE MAINTENANCE (FFP)

Tasks performed in support of this task order require management oversight, communications, time management, quality assurance and control, risk management, configuration management, cost management, and software integration. Using state-of-the-art knowledge, skills, tools, and techniques, the contractor shall:

5.1.1 Provide a Project Management Plan (PMP) that describes the proposed management approach, the milestones, tasks, and subtasks required by the task order. The PMP shall provide for an overall Work Breakdown Structure (WBS) and associated responsibilities. The Project Manager shall be responsible for a detailed PMP that identifies and assigns tasks, major milestones, dates and dependencies, and indications of critical path. The PMP shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. The Government approved PMP will be used to monitor the Contractor's progress. The PMP is an evolutionary document, any revisions are considered incorporated upon written acceptance of the Government, inclusive of any changes to deliverables detailed in the PMP. The PMP shall be entered and maintained in Enterprise Project Server.

5.1.2 Provide information and recommendations to respond to Congressional, DOD, other Government agency, media or industry inquiries, Freedom of Information Act (FOIA) requests, audits and for Congressional testimony.

5.1.3 Maintain a real-time calendar of ongoing projects this includes maintaining, refining, and revising the project collaboration sites currently on SharePoint or other

Government-designated repositories. This site must include project overview documents, a consistently updated document library that preserves document history, schedules, a dashboard, assignment and POC lists, summaries and agenda for all meetings and conferences attended, and support for collaborative editing/versioning of project documents.

5.1.4 Coordinate with all impacted DMDC governance bodies such as DMDC Information Systems Security Group (DISSG), Architecture Review Board (ARB), Executive Governance Council (EGC), Enterprise Quality Assurance (QA), Configuration Management (CM), IT Operations, Consolidated Call Center (CCC), DMDC Management Advisory Group (DMAG), production support, implementation support, and other impacted divisions for project requirements and execution for approval authority.

5.1.5 Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage. Current BPR tools include Sparx Enterprise Architect, Microsoft Project Server, and Change Gear but could change throughout the life of this order.

5.1.6 Monitor legislative and policy changes; perform regulatory, legislative, policy and standards research and provide assessments to the government of impact to designated programs and IT products; and implement government directed legislative and policy changes.

5.1.7 Prepare ad-hoc white papers, information papers, point papers, presentations, briefings, business process assessments, and system assessments. Ad-hoc research requests to include performing special studies, conducting data research and respond to inquiries from DMDC customers.

5.2 TASK 2 – PERFORM SOFTWARE DEVELOPMENT MAINTENANCE SERVICES (SDMS) (TIME & MATERIAL)

Software sustainment involves orchestrating the processes, practices, technical resources, information, and workforce competencies for systems and software engineering, to enable systems to continue mission operations and also be enhanced to meet evolving threat and capability needs. Software sustainment activities can include correcting known flaws, adding new capabilities, updating existing software to run on new hardware and updating the software infrastructure to make software maintenance easier. The contractor shall perform all work using best software sustainment and commercial business practices, but not contradict Government business practices. Adhere to established software development standards and guidelines as prescribed by Capability Maturity Model (CMM), Capability Maturity Model Integration (CMMI), Institute of Electrical and Electronics Engineers (IEEE), and International Organization for Standardization (ISO) and DMDC Software Development instruction (Appendix B).

The Government will provide Application/Product Roadmaps (Appendix A) that detail the direction of the product and the work required to get there. The roadmap is used to communicate the product direction and progress to internal teams and external stakeholders. Roadmap priorities shall be established by the Service Delivery Product Owner. Releases for the period of performance are reflected in the PWS and/or Appendix A. Releases listed on the Roadmap are estimated and scheduled within a calendar quarter but may be more frequent than quarterly. Additional quarterly releases will be managed based on DMDC priorities. The program requirements may vary from quarter to quarter but will not exceed the overall number of releases identified for the period of performance.

5.2.1 Support an agile development methodology (rapid development); software products shall be modular and reusable; sustain software capabilities in a manner that is responsive to immediate and future user needs.

5.2.2 Reduce and eliminate redundant tasks for sustainment efforts across all supported systems; e.g., develop software fixes in a manner that can be applied to multiple systems and consolidate management resources, functions, and tasks.

5.2.3 Create and update functional and technical specifications, design documentation, program specifications, unit test criteria, code and test program units, and produce program documentation.

5.2.4 Provide Tier Level 3 support (24/7/365) for application outages in production and data issues escalated by the Customer Contact Center (CCC), program manager, or application helpdesk.

5.2.5 Update applications and infrastructure in support of DMDC infrastructure improvements, changes, technical refreshes, or migrations (e.g., Common Update Framework (CUF), AION migration, Data Center location transition). Assist the government in converting and testing software to run on new hardware or virtualization platforms.

5.2.6 Develop and execute Software Test Plan(s) to address application or system use cases, user interfaces, security considerations, and reports using test data designed to demonstrate compliance with all documented functional specifications for each release.

5.2.7 Test software changes integrated with the existing software and/or other systems to verify that corrections and/or enhancements to software were successfully implemented and do not adversely affect any other components of the system or other systems.

5.2.8 Identify, plan, and conduct corrective, preventative, and adaptive maintenance

5.2.8.1 Perform corrective maintenance activities including the identification, isolation, and resolution of system problems to restore normal operations.

5.2.8.2 Perform preventative maintenance activities including systematic inspection, detection, and correction of problems before they occur to increase software maintainability and reliability, and to prevent problems in the future (e.g., applying application or operating system patches).

5.2.8.3 Schedule preventive maintenance, apply patches, and adhere to information assurance vulnerability alerts as well as planning for and management of multiple landscapes and transport paths and coordination across and support for multiple products/programs.

5.2.8.4 Perform adaptive maintenance activities designed to cope with changes in the software environment including the implementation of processing efficiencies, and/or considerations for additional delivered capabilities to enable existing and evolving requirements.

5.2.8.5 Implement methodologies and approaches to establish consistency in sustainment activities, develop preventive measures and document issue resolution procedures.

5.2.8.6 Provide day-to-day oversight of sustainment teams with emphasis on analysis, coding, testing, documentation, acceptance and maintenance phases.

5.2.8.7 Analyze root causes of operational malfunctions and coordinate resolutions, participate in escalated issues, address customer issues, and follow-up on outstanding issues.

5.2.8.8 Recommend process improvements to improve operational efficiency and develop standard operating procedures and knowledge base solutions.

5.2.8.9 Create and maintain a Software Maintenance and Development Plan (SMDP) that defines the approach, timeline and steps by which the development and maintenance of software applications will be accomplished and the management approach to software development and maintenance. The SMDP shall address software and sustainment processes, methods, organizational responsibilities, tools, configuration management, software quality, metrics, and other activities relevant to accomplish the requirements of the PWS. The plans shall be revised and updated as necessary to remain current and effective.

5.2.9 Application Information Security

5.2.9.1 Deliver software that meets the requirements of DoD and DMDC Information Assurance (IA) policy. Software shall be secure, accreditable and ensure security requirements are

addressed in software design and development. Personnel performing IA activities shall obtain and remain current with, required technical and/or management certifications.

5.2.9.2 Ensure application code is updated with the latest security patches to minimize security vulnerabilities and provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with current DODI 8510.01; Risk Management Framework (RMF) for DOD IT. Provide documentation as requested to support RMF Certification and Accreditation processes.

5.2.9.3 Implement procedural countermeasures and Government-issued technical advisories including Security Technical Implementation Guides (STIGs), service packs and security patches according to Automated System Security Incident Support Team (ASSIST) guidance within the timeframe specified by the technical advisory when such notices directly apply to the application software code used or developed. Report monthly completion of all Government issued technical advisories as described in this paragraph to the Information Assurance Officer.

5.2.9.4 Develop and implement a Software Security Risk Management Plan to assess and manage risk and coordinate with the Information Assurance Officer.

5.2.10 Unit Testing

5.2.10.1 Developers shall write unit tests to ensure that the unit (be it a method, class, or component) is operational and test across a range of valid and invalid inputs. In a continuous integration environment, unit tests shall be conducted anytime there a change to the source code repository.

5.2.10.2 Conduct a verification of the interaction one or more new or modified coded product components, as well as dependent components that have not been modified, to ensure complete coverage of requirements and successful interaction of components prior to full system testing.

5.2.10.3 Conduct interface (system-to-system), stress and volume testing, as part of development testing to identify issues as early as possible, reducing the risk and cost of rework.

5.2.10.4 Create test data in all testing environments.

5.2.10.5 Version and maintain all test artifacts in order to perform repeatable and reliable testing.

5.2.10.6 Develop test plans, data and tools that exercise the application at both the unit and systems integration levels.

5.2.10.7 Provide draft project artifacts to Enterprise Quality Assurance (QA) no later than two weeks prior to the anticipated QA start date; artifacts include: Requirements Traceability Matrix (RTM), Functional Specifications, and Release Notes. The contractor shall revise QA release notes after submission, based upon unknown variables that emerge during development.

5.2.11 Release Management

5.2.11.1 Manage and plan all software releases; assess and manage risk and resolve issues that affect releases as they move forward. Communicate release details and schedules within fall DMDC environments. Continually work to make the release process better, faster and set a solid foundation that evolves.

5.2.11.2 Manage system software, hardware, and configurations, to include patches, emergency data fixes, and upgrades for each release. Inform system users of upcoming releases that will change or increase system functionality or capability.

5.2.11.3 Ensure each release is compliant with Risk Management Framework requirements to gain certification as required by DoD Information Assurance and DMDC policies. Ensure monthly Information Assurance Vulnerability Alerts (IAVA) issues are monitored and resolved. Coordinate new releases with stakeholders, hosting facility and owners of connected systems. Coordinate with and allow system access to the Government IA representative for routine testing and data collection as necessary or requested to comply with IA requirements to obtain or retain Authority to Operate.

5.2.11.4 Maintain a release log, build and release procedures, dependencies and notification lists.

5.2.12 Application Level Change Management

Manage and maintain the existing automated software build and deployment infrastructure for each deployed application in support of the following environments: stand-alone workstations, Local Area Network/Wide Area Network (LAN/WAN) development, LAN/WAN Test, and LAN/WAN Quality Assurance (QA). This includes but is not limited to overseeing the source code repository, infrastructure, common library components, and scripts required to perform CM automation. Coordinate with DMDC Release Planning to monitor, coordinate and stage required artifacts for each scheduled release. Software shall be staged based on scheduled and out of-cycle release planning in support of the following environments. The environments may include the following: stand-alone workstations, LAN/WAN networks, Contractor Test, Stress Test and Production. Government review and approval is required prior to promoting to production environments. Provide a pre-deployment checklist to ensure all software is accounted for in each release and process change requests managed through the DMDC Configuration Management infrastructure.

5.2.13 Configuration Management (CM)

5.2.13.1 Develop and maintain a configuration management plan (CMP) that tracks and controls changes in software to include revision control and the establishment of baselines. The CMP is a dynamic document, and shall be updated as work proceeds and the necessity arises.

5.2.13.2 Identify, define and baseline configuration items (CI)

5.2.13.3 Control modifications and releases of CIs; record status of Cis and any modifications ensuring consistency and completeness

5.2.14 Production Support

5.2.14.1 Monitor process and software changes that impact production support, communicate project information to the production support staff and raise production support issues to the product owner. Support scheduled and unscheduled, on-request and end-user initiated processing of business applications.

5.2.14.2 Maintain a run log for all batch applications. Implement procedures for proactively identifying, preventing, and responding to problems. Provide ongoing running and monitoring of batch systems, such as the personnel data feeds, Security, Point in Time and Database Extract.

5.2.14.3 Maintain and support all Test, Model Office, user acceptance test, benchmark test, stress test, and Production regions, including systems and applications components Support updates and monthly loads of address validation software.

5.2.14.4 Develop and maintain Disaster Recovery Activity (DRA) and Continuity of Operations (COOP) plans for every required application and interface.

5.2.14.5 Provide escalation support to understand, troubleshoot, root cause, log analysis and resolve complex technical issues.

5.2.14.6 Provide daily support with resolution of escalated tickets and act as liaison to product and technical leads to ensure issues are resolved in timely manner. Communicate with source of escalation, complete appropriate documentation, and process tickets according to agency methodology.

5.2.15 Requirements Traceability Matrix (RTM)

Create or update Requirements Traceability Matrix for all projects/products. The RTM shall clearly link the new and/or changed requirements to where and how they have been

implemented in the system. The RTM shall provide backwards and forward traceability documenting each requirement from its source through definition, analysis, design, testing, acceptance, and deployment.

5.2.16 Cyber-Security & Information Assurance (IA)

5.2.16.1 Ensure that all system or application deliverables meet the requirements of DoD and DMDC Information Assurance (IA) policy and that personnel performing IA activities obtain, and remain current with, required technical and/or management certifications. Protect system information and resources according to established security policies and procedures and ensure application code is updated with the latest security patches to minimize security vulnerabilities.

5.2.16.2 Provide documentation and confirm that application code changes comply with the DoD system security policy and are properly certified and accredited in accordance with DODI 8510.01; Risk Management Framework (RMF) for DOD IT, signed 12 Mar 2014. The Contractor shall be consistent with established disciplines and best practices for effective systems engineering, systems security engineering, and program protection planning outlined in DoDI 5000.02.

5.2.16.3 Provide documentation to support RMF Certification and Accreditation processes. Final approval for all IA tasks under this contract belongs to the Information Assurance Officer, Cyber Security Branch. The contractor shall obtain final approval for all IA-related design decisions, including cryptography, authentication, access control, data transfer and storage, Need-to-Know (NTK), or other IA technologies that must be coordinated with and approved by Cyber Security Officer.

5.2.16.4 Identify potential program, system, and engineering risks that pertain to cyber security; and participate in and support the development of risk mitigation plans and monitoring of risk mitigation activities.

5.3 TASK 3 – CONDUCT BUSINESS REQUIREMENTS ANALYSIS (FFP)

Business requirements analysis is a comprehensive declaration of what the project is supposed to achieve and a step-by-step procedure to discover, analyze, and document the essential requirements connected to the product. Business analysis involves frequent communication with system users to determine specific feature expectations, resolution of conflict or ambiguity in requirements defined by the various users, avoidance of feature creep and Identification of possible technical solutions and best value alternatives.

5.3.1 Conduct requirements analysis, feasibility, migration, business process reengineering, requirements validation through interaction with functional proponent, requirements traceability, business process modeling, rules, data requirements, and interface management. Document workflow, business processes, data and services, and include a

standard set of artifacts for the purpose of understanding the program asset/software requirements.

5.3.2 Collaborate with stakeholders to formulate and communicate requirements; prepare a business requirements document (BRD) that details the solution documenting customer needs and expectations. Conduct requirements and design walkthroughs with external and internal consumers.

5.3.3 Translate requirements to design modifications maintaining the integrity of the product's design, develop user scenarios and interfaces.

5.3.4 Provide business process-improvement support that includes all activities involved in helping improve customer data systems through business processes including rethinking program design and aligning information technology infrastructures with business missions, goals, and objectives.

5.3.5 Create data flow diagrams, perform data standardization and perform enterprise modeling, functional economic analysis, simulation/modeling, activity based costing and activity based management support.

5.3.6 Provide "as is "and "to-be" functional analysis.

5.3.7 Software and Systems Integration & Implementation

5.3.7.1 Facilitate and monitor the integration, interoperability, and synchronization of enterprise-wide systems and infrastructure solutions and services.

5.3.7.2 Develop a systems integration plan to oversee the development of external dependent projects and provide a strategy for the successful integration of all software and hardware into the environment. Plan to include roles and responsibilities, assumptions, internal and external stakeholders, integration/coordination with external organizations, implementation schedules and status, interdependencies of applications, systems integration, design review and acceptance procedures and schedules, user acceptance testing support, privacy and security management (site security, data privacy/security), and defect tracking and resolution.

5.3.8 Software Transition Support

The Contractor shall provide support for transition of the delivered software components to the Government or Government-specified Contractor, to include, but not be limited to, performing software test and verification, training, and corresponding documents that provide information on the use and maintenance of the software and its components. The Contractor shall prepare a project specific Software Transition Plan. The Software Transition Plan shall address products to be turned over (documentation, software, hardware, tools), formats and media, schedules,

and support during transition. The Contractor shall include all resources needed to control, copy, and distribute the software and its documentation. The Contractor shall identify at the Test Readiness Review all hardware and software that will be transitioned during each delivery and the time frame of the transition.

5.4 TASK 4 – CONDUCT DATA QUALITY MANAGEMENT (DQM) (FFP)

Data Quality Management in the DoD is essential to mission success. It ensures that quality data supports effective decision making and that the correct data gets to the right person at the right time. DMDC requires Data Quality Management that incorporates a cycle in which continuous observation and improvement leads to improvement in the quality of data assets across the enterprise. Data quality management responsibilities fall under the DoD information management and data administration initiatives (DODD 8000.1 and DODD 8320.1).

Conduct data quality assessment using data profiling to identify the degree to which poor data quality impedes business objectives and prepare a DQ assessment report

5.4.1 Define business related data quality and validity rules; perform measurements and set performance targets

5.4.2 Design quality management processes that remediate process flaws

5.4.3 Inspect, monitor and remediate when quality of data is not acceptable.

5.4.4 Automate data quality with tools such as:

- edit checks
- reports
- automation of functions to evaluate quality of data

5.4.5 Produce a Data Quality Implementation Plan that establishes processes and procedures in line with DoD and organization goals.

5.4.6 Provide a means to identify, track, and report non-conforming data and recommendations on preventive and corrective actions to improve data quality.

5.4.7 Provide a monthly report of the status of data quality and produce metrics indicating the quality of data.

5.4.8 Provide data cleansing efforts that correct existing data quality issues and improve future data quality.

5.4.9 Research and analyze on TASS and PDR data discrepancies from the monthly data pull reports.

5.4.10 Benefits Error Analysis

The Government estimates the volume of daily personnel transaction files to include 10 active duty files per day; 14 Reserve Components Common Personnel Data System (RCCPDS) files per day; up to 10 Guard Reserve Initial Duty (GRID) files per day (Reserve/Guard components do not send a file every day); and 7 Guard Reserve Active Service (GRAS) Analysis Report files daily.

5.4.10.1 Review daily transactions rejected in the batch processes with primary focus on Personnel Finance Transfer (PFT), GRAS, and GRID to include handling rejects, documenting fixes and tracking volumes. Correct not less than an average of 100 errors daily and complete the following actions:

- Determine root cause and appropriate response
- Coordinate with the service liaisons
- Make recommendations for corrective actions

5.4.11 Medical Satellite (MedSat) and Person Data Repository (PDR) Benefits

5.4.11.1 Develop internal data quality scripts that produce high quality data leading up to the data conversion activities; the government estimates 30 errors per day that require intervention.

5.4.11.2 Ensure all data discrepancies that would negatively impact the data conversion are resolved; it is expected there are less than 10 categories of errors that will negatively impact the data conversion activities.
5.4.11.3 Analyze and resolve data discrepancies and anomalies identified through internal quality control monitoring.
5.4.11.4 Review and update data conversion scripts, correspondence, carry forward drive time waivers; correct handling of PCM assignments, and region changes.

5.5 TASK 5 - OPERATE The Common Access Card (CAC) Central Issuance Facility (CIF) (FFP)

The Common Access Card CIF is the Department of Defense's (DoD) enterprise solution for bulk production and issuance of CAC cards and their PINs for more than 200,000 new recruits and other DoD personnel annually by collecting required demographic and identity information, processing that data to produce the cards centrally, and shipping the cards to pre-determined locations including eight basic training sites, three academy sites, and two officer training schools.

5.5.1 Operate and maintain the CIF Pre/Post Process Server (PPS) Client Software which drives the creation and printing of the CAC Cards including:

- Process bulk submission requests and data.
- Process cards for encoding.
- Load CAC holder certificates onto the card.
- Load CAC holder photo and other standard biometric information onto the card.
- Set the card's PIN.

- Print the card.
- Seal the card in the DMDC approved confidential packaging for shipping.
- Ship the card to the CAC holder at the designated location.
- Print the PIN and seal it in a confidential mailer from a separate physical location.
- Ship the confidential mailer containing the PIN to the CAC holder at the designated location, in accordance with DoD and DMDC guidelines.

5.5.2 Deliver CACs and PINs to the designated location within timeframes listed in the chart below. There shall be zero deviations from the Service Level Agreements (SLA) with the customers and all deviations will be coordinated with the customer location once it is known that the SLA will not be met. All shipments shall be made using the Government shipping account. All shipments shall be made using the most cost-effective shipment method that will still meet the delivery SLA.

Service/Site	Timeframe
Army	Next business day for CACs and no later than two business days for PINs
Marine Corp	No later than five business days for CACs and no later than five business days for PINs
Navy, Air Force & Service Academies	No later than three business days for CACs and no later than three business days for PINs

5.5.3 Provide a monthly CIF Operations Report that provides SLA deviations, explanations for the deviation, remediation actions and actions taken to prevent future deviations. Report shall also include total CAC production, issues, risk and remediation.

5.5.4 Perform maintenance and updates to the CIF environment, printers and all CIF components following DOD and DMDC procedures.

5.5.5 Coordinate with Enterprise Quality Assurance to conduct test runs and changes utilizing the CIF test environment and the bulk printing components. Verify the results.

5.5.6 Maintain physical control of smartcard stock and other consumables present in the CIF; ensure physical and logical access controls to the Secure CIF environment are followed.

5.5.7 Document all issues using the DMDC approved tool for prioritization and scheduling

5.5.8 Collaborate and provide support to CIF vendors and stakeholders.

5.5.9 Conduct maintenance, integration, installation and testing and diagnostic support of the CAC Infrastructure components
- Profile Studio/Profile Manager (PS/PM)
- Key Management System (KMS)
- Inventory Logistics System (ILS)
- Card Content Server (CCS)
- Exchange Manager (EM)

5.5.10 Maintain, update and operate the User Portal (CCS, 4tress Profile Manager/Profile Studio) on the Issuance Portal and Post Issuance Portal and the Inventory Logistics System Non-classified Internet Protocol (IP) Router Network (NIPRNet) tokens.

5.5.11 Support the RAPIDS CAC infrastructure, incidents and outages and CAC components (CCS, KMS, ILS, PS/PM & EM) 24x7x365. Support services include Production and Disaster Recovery Regions Support (24x7x365) in all TEST, MODEL and Production environments.

5.5.12 Include all defects and issues in the Monthly Status Report (MSR). Historically there have been 0 - 5 SRT calls per month per Credentialing/Identity Management applications.

5.5.13 Maintain valid production encryption keys used in TEST, MODEL, Production and Disaster Recovery environments through the operation of the Key Management System.

5.5.14 Perform security patching, analyze and mitigate Information Assurance Vulnerability Alerts (IAVA).

5.5.15 CAC Testing Support (OPTIONAL) (TIME & MATERIAL)

The DoD Test Common Access Card Request (TCR) is used to obtain test CACs to assist in the development of applications. RAPIDS issues test CACs and Alternate Logon Token Issuance & Management System (ATIMS) for issuance of Alternate Logon token request. All new identities shall be created in the test instance of Defense Enrollment Eligibility Reporting System (DEERS). The contractor is responsible for packaging and shipment of the test tokens. Shipments shall be recorded and logged.

5.6 TASK 6 – SUPPORT THE NON-COMBATANT EVACUATION OPERATIONS TRACKING SYSTEM (NTS) & EMERGENCY TRACKING ACCOUNTABILITY SYSTEM (ETAS) (FFP)

The Government estimates six (6) major software releases annually

5.6.1 Sustain and enhance NTS/ETAS applications including online and offline capabilities (Appendix A); integrate new technologies and requirements from the NTS/ETAS user community. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.6.2 Remediate vulnerabilities and security findings in production and update Plan of Action and Milestones (POA&M) to capture how the determination was addressed.

5.6.3 Evaluate and test new and existing hardware (e.g. scanners, printers, tablets, and webcams) and software with test cases to ensure full functionality. Integrate hardware and ensure legacy hardware continues to function with each release. Estimate level of effort for integration for Government approval.

5.6.4 Demo the NTS/ETAS software to the Government product owner and Service Delivery Branch Chief before releasing to Enterprise QA.

5.6.5 Conduct troubleshooting of the NTS/ETAS web application in development and production.

5.6.6 Assist and provide expertise with audits and data calls.

5.6.7 Travel and participate in DoD exercises twice a year to OCONUS/CONUS locations.

5.6.8 Provide Tier III support for hardware, software, database analysis, data quality issues and configuration outages across all DMDC deployment regions.

5.6.9 Update and maintain currency of the NTS artifacts and User Guide based on customer and DMDC feedback

5.6.10 Develop the capability to remotely deliver software installation files to a permanent locations so NTS POCs have constant file access.

5.6.11 Research new software and hardware technologies that provide solutions to problem sets, determine feasibility of integrating into the application, and estimate the level of effort for integration into NTS/ETAS.

5.6.12 Coordinate with DoD and federal agency partners requesting access to the NTS system and reports.

5.6.13 Maintain and update the NTS Information website.

5.7 TASK 7 - Enhance and Sustain the Automated Central Tumor Registry System (ACTUR) (OPTIONAL) FFP

ACTUR is a tri-service application, which collects and reports on data from Army, Air Force, and Navy facilities. The ACTUR application is currently used at over one hundred Military Treatment Facilities (MTFs) throughout the U.S., Europe, and the Far East. The main goal of ACTUR is to provide appropriate information to numerous cancer research organizations, like the American College of Surgeons (ACoS) Commission on Cancer (CoC) that utilize the National Cancer Database (NCDB).

The user base consists of roughly 120 users worldwide and the application is responsible for about 4,000 transactions per day. ACTUR includes the ACTUR Manager, ACTUR Web Application, and ACTUR Reports.

5.7.1 Provide an ACTUR Project Management Plan (PMP) that identifies and assigns tasks, major milestones, dates, dependencies and indications of critical path. The PMP will include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as technical content review. Tasks from the final and Government approved PMP shall be selected as milestones against which Contractors' progress shall be monitored. The PMP is an evolutionary document that shall be updated annually and identify tasks and deliverables specified in operating procedures that shall be completed by the contractor. Any updates to the PMP shall be incorporated to the task order upon Government approval.

5.7.2 Provide end-user support for problems or defects with ACTUR products

5.7.3 ACTUR REPORTING

5.7.3.1 Develop, maintain, and implement quality control procedures for ad-hoc and recurring data requests and reports. Produce the following reports:

- National Cancer Database (NCDB) report
- North American Association of Central Cancer Registries (NAACCR) cancer report
- Ad-Hoc state agency reports
- Rapid Quality Reporting System (RQRS) to Army, Navy and Air Force

5.7.3.2 Conduct twice- weekly "NCDB Data Pull"

5.7.3.3 Migrate ACTUR Reports from COGNOS to SAS

5.7.3.4 Attend the Monthly ACTUR User Group Meetings

5.7.3.5 Provide the Center for Cancer Research (CCR) data reports

5.7.3.6 Provide a monthly activity/status report that includes the following:

- Complete & Incomplete Case Status Report
- Data Submission Report
- Data Sub-report

5.7.3.7 Conduct Site Security Management (SSM) provisioning new users in both ACTUR Web and the ACTUR Reporting tool.

5.7.4 Conduct ACTUR SW Sustainment & Enhancements

5.7.4.1 Conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance.

5.7.4.2 Add, modify, and delete functionality based on customer requirements.

5.7.4.3 Conduct quarterly maintenance releases that include security updates to the application.

5.7.4.4 Implement procedures for proactively identifying, preventing, and responding to problems.

5.8 TASK 8 – SPECIFIC SUSTAINMENT REQUIREMENTS (FFP)

This section relates to the specific products and applies to the applications as a group.

5.8.1 Sustain and enhance the Real-Time Automated Identification System (RAPIDS) Application Suite - (The Government anticipates 4 major releases annually) See Appendix A for products and release data.

5.8.1.1 Migrate RAPIDS to WebLogic 12c.

5.8.1.2 Conduct a technology refresh of RAPIDS dependent components (Java, ActivClient middleware, PDF form viewer).

5.8.1.3 Remediate and execute tasks identified on the product owner prioritized list for JIRA maintenance.

5.8.1.4 Integrate next model camera with Aware PreFace.

5.8.1.5 Sustain and maintain the use of Probabilistic Search in RAPIDS.

5.8.1.6 Support the development and testing for implementation of the DoD Next Gen USID card.

5.8.1.7 Develop and test requirements for Foreign Affiliate Lockdown and surrogate additions; support DS Logon transition from Security Online to EMMA for user provisioning.

5.8.1.8 Sustain and enhance RAPIDS applications; integrate new technologies and requirements from the RAPIDS user community.

5.8.1.9 Evaluate and test new and existing hardware (e.g. scanners, printers, tablets, and webcams) and software with current test cases to ensure full functionality. Integrate hardware and ensure legacy hardware continues to function with each release. Estimate level of effort for integration.

5.8.1.10 CAC Pin Reset

5.8.1.10.1 Migrate to WebLogic 12c.

5.8.1.10.2 Conduct a technology refresh on dependent components (CCS 5, Java, ActivClient middleware, PDF form viewer).

5.8.1.10.3 Configuration Management Tool.

5.8.1.10.4 Conduct bug remediation and resolve urgent updates with each RAPIDS release.

5.8.1.10.5 Sustain and document the Satellite Access Service (DSAS) applications.

5.8.1.10.6 Migrate Message of the Day to WebLogic 12c.

5.8.1.10.7 Sustain and enhance Rapids Logon Monitor (RLM) application.

5.8.2 Trusted Associated Sponsorship System (TASS) - (4 Major releases annually)

5.8.2.1 Conduct research, analysis, and troubleshooting to resolve production issues.

5.8.2.2 Support enterprise software & hardware; complete development tasks to support DMDC Enterprise software and hardware changes, includes but not limited to new hardware, software migrations.

5.8.2.3 Complete development tasks associated with high and medium priority backlog JIRA tickets.

5.8.2.4 Conduct bug remediation and resolve urgent updates of the Verifying Official Information System (VOIS) with each RAPIDS release.

5.8.3 Infrastructure Support - (4 Major releases annually)

5.8.3.1 Conduct bug remediation of the Audit server and resolve urgent updates with each major release of RAPIDS.

5.8.3.2 Migrate Bulk Certificate Revocation to WebLogic 12c.

5.8.3.3 Support, develop and test the Web Based Bulk Revocation (WBBR) interface.

5.8.3.4 Sustain the Token Issuance Infrastructure.

5.8.3.5 Transition functionality of Site Maintenance Tool (SMT) to ID Card Office Online (IDCO) 3.0 and migrate to WebLogic 12c. The Government estimates two (2) releases annually.

5.8.4 Application Security Suite (FFP) reference Appendix A for roadmap and product list- (The Government estimates 4 Major releases and 4 Minor releases annually)

5.8.4.1 Sustain and enhance Application Security Suite (appendix A) applications; integrate new technologies and requirements. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.8.4.2 Enterprise Management & Monitoring of Accounts (EMMA) Web User Interface (UI) Framework.

5.8.4.3 Migrate Enterprise Management & Monitoring of Accounts (EMMA) Web User Interface Angular.

5.8.4.4 Update ASIS/COAL to require a valid DoD PIV authorization certificate at logon by January 31, 2020 as per DOD CIO memo 'Modernizing the Common Access Card – Streamlining Identity and Improving Operational Interoperability' dated December 7, 2018.

5.8.4.5 Conduct bug remediation and resolve urgent updates with each security suite release.

5.8.4.6 Modify EMMA web site to include search functionality.

5.8.4.7 Monitor and respond to JIRA tickets submitted to its queue. There were a total of 511 tickets submitted during the last 12 months.

Ticket Action	Timeframe
Triaged/assigned (100%	Within 2 Business Days
Resolved (90%)	Within 10 Business Days
Escalated	If ticket cannot be resolved within 10 business days, it will be escalated to government lead.

5.8.5 **Defense Enrollment Eligibility Reporting System (DEERS)** - Conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance for all applications and products in accordance with Appendix A. The major subsections are:

5.8.5.1 **Veterans Affairs Benefits (Education & VLER) releases)**

5.8.5.2 **Benefits & Entitlements**

5.8.5.3 **Infrastructure Support**

5.8.5.4 **TRICARE Enrollment**

5.8.5.5 **TRICARE Eligibility & Claims**

5.8.6 Identity Web Services (IWS) Suite of Applications

5.8.6.1 Sustain and enhance Internet Web Services Suite of Applications (Appendix A); integrate new technologies and requirements. Conform to DMDC mandated technology and ensure the system in is compliance within the required timeline.

5.8.7 Provide HID SME support in support of HID products used in the RAPIDS Suite.

5.9 **TASK 9 – CONDUCT FACIAL RECOGNITION ANALYSIS (OPTIONAL) FFP**
The Government anticipates four (4) releases annually

Provide program management support to include support of a facial recognition Office. Assist the Government in the planning, implementation, maintenance, and operation of the Facial Recognition Software Automation Implementation capability.

5.9.1 Analyze Facial Recognition data utilizing DMDC data. The contractor shall consult with DMDC stakeholders for requirements. The analysis shall consist of:

- Analysis of specifications and programming approaches
- Analysis of incoming data to ensure compliance with technical specifications and quality standards for various initiatives
- Collaboration with data submitters to manage all facial recognition requests
- Communicate corrections and recommend remediation to improve requests for proper submittal/acceptance by DMDC

5.9.2 Respond to Facial Recognition requests from customers within 10 days of receiving the request. Manage the data request through DMDC Data Request System (DMDCRS) and provide monthly analyze of the number requests received.

5.9.3 Conduct business analysis and post-production release support; communicate with software vendor on bug analysis, correction, verification and implementation, performance metrics and standard operation procedures.

5.9.4 Document application architecture.

5.10 TASK 10 – AUTOMATE FACIAL RECOGNITION (OPTIONAL) (TIME & MATERIAL)

5.10.1 Conduct the system and integration activities such as requirements, design, development and internal development testing for TacID software and scope future enhancements for application automation.

5.10.2 Produce a technical design to specify the technical architecture, technical functionality; user interfaces and interfaces as required by the application automation phase of the product.

5.10.3 Prepare and execute milestone reviews for requirements, design, development and testing as required by the DMDC lead, to ensure the development meets the needs of the Government. The milestones shall be outlined in the government approved project management plan.

5.10.4 Update the COTS product into DMDC's infrastructure.

5.10.5 Assist in documentation of the application architecture for the DMDC Architecture Repository.

5.10.6 Provide documentation for functional and technical specifications, data quality reviews, mission security assessments and mission impact assessments; Investigate, prepare and execute milestone reviews for requirements, design, development and testing.

5.10.7 Analyze specifications, formulate programming approaches, and consult with DMDC and its customers to clarify requirements.

5.10.8 Analyze incoming data to ensure compliance with the required technical specifications and quality standards for various initiatives.

5.10.9 Collaborate with data submitters to manage all data intake. Communicate corrections and recommend any remediation to improve the data analytical value.

5.11 TASK 11 Common Update Framework (CUF) (FFP)

5.11.1 CUF (Four major releases)

5.11.2 Sustain and maintain CUF, conduct all phases of software maintenance as defined in ISO/IEC 14764. Possible categories are corrective maintenance, adaptive maintenance, perfective maintenance, and preventive maintenance.

5.11.3 Continue the work on CORE to CUF migration, work with all CUF client applications to migrate them to the new data access processor being modified within 6-months of the new processor being deployed to production.

5.11.4 Separate the CUF-EJB application into two separate components—one component for the web service and one component for the CUF dashboard

5.12 TASK 12 SUPPORT ACCOUNTABLE CARE ORGANIZATIONS (ACO) DEMONSTRATION

5.12.1 ACOs are high value providers who offer a range services to their enrollees. TRICARE is testing ACOs as primary care providers for its non-Active Duty Service Member populations. The ACO provider type will operate similarly to the US Family Health Plans (USFHP) Designated Providers. Coordinate with the Defense Health Agency (DHA) to complete the following tasks:

5.12.2 Design and implement features to support integration of a single Accountable Care Organization (ACO) within the Prime program. Update enrollment applications as needed to support identified business requirements. Must be in Production NLT 1 Nov 2019 to support start date of 1 Jan 2020.

5.12.3 Create a new provider type or leverage existing provider types. Create an enrollment fee waiver for beneficiaries participating in DHA's ACO Demonstration project. The waiver shall be manually applied initially, but should be designed to be automatically applied and maintained based on business rules related to enrollment in the ACO Demonstrations or related efforts. The waiver shall operate similarly to the Medicare waiver. Provide options for applying the waiver to additional demonstration projects.

5.12.4 Support generic clinic level Primary Care Manager (PCM) for demonstration participants to include loading the PCM

5.12.5 Develop and implement changes to self-service and operator applications to support new ACO enrollment and fee waiver requirements.

5.12.6 Develop and provide data to support beneficiary mailings; modify correspondence rules to prevent automatic beneficiary notifications.

5.12.7 Coordinating with DHA develop; provide recurring ACO enrollment, disenrollment and waiver reports.

5.12.8 Provide necessary documentation (including external specifications and data dictionary) and demonstration/training.

6.0 TASK 13 – PROVIDE PLANS, REPORTS, AND DOCUMENTATION (FFP)

6.1 Monthly Status Report (MSR) and Senior Management Reviews (SMR)
The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ

6.2 Meeting Summaries
The Contractor shall follow the Meeting Summaries requirements identified in the PWS Section 5.8.4 of the EITS II Base IDIQ

6.3 Weekly In-Progress Review (IPR)
The Contractor shall follow the IPR requirements identified in the PWS Section 5.8.5 of the EITS II Base IDIQ

6.4 Problem Notification Report (PNR)
The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.5 Expenditure Resources Report

6.5.1 Provide an Expenditure and Resource Report (ERR) to the DMDC COR on a monthly basis. The Contractor shall submit the quarterly ERR by the twenty-fifth (25th) calendar day of the month after the end of the month for services rendered. This report shall be detailed by each project/product that is being worked by the contractor in support of this PWS, the amount that will be billed to the Government and the resources (hours and personnel) assigned to that task. Each report shall provide the current month and cumulative task order costs breakout as a monthly subset by project organized by line item, with a total at the end of the row for the particular application/product/project.

6.5.2 The report shall link all products related to a specific application, with a roll up on the total cost for a particular application if applicable. (For example RAPIDS as a top line and all products that are part of RAPIDS linked to RAPIDS showing a total effort for RAPIDS suite of applications, Facial Recognition on the other hand would stand alone since there are no other products lined to that application).

6.5.3 The report shall separate sustainment costs from enhancement costs, and organized by line item.

6.5.4 The report shall separate FFP from time and material costs and be organized by line item.

6.6 ORIENTATION/POST AWARD CONFERENCE

The Contractor shall follow the Orientation/Post Award requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ

6.7 **DELIVERABLES**

The Contractor shall submit a draft version of each deliverable and the government will provide written acceptance, comments and/or change requests, if any, in accordance with PWS Section 7.0. The Contractor shall make any corrections and submit the final deliverable to the contractor established and maintained approved site location (currently Sharepoint), in accordance with the dates listed in the following table and in accordance with PWS Section 7.0:

PWS Section	Deliverables	Date Due/Frequency
5.1.1	Project Management Plan (PMP)	Draft submitted within 20 work days of order award; Final submitted within ten days after receipt of Government comments. Updates as needed and no less frequently than 30 days after exercise of an Option Period.
5.1.3	Maintain SharePoint Site	Updated 5 days after award and updated within 2 days after documents change
5.1.3	Project Documentation	30 days after award and updated within 2 days after documents change
5.1.4	DMDC Governance approvals	Per Government approved PMP
5.2.8.9	Software Maintenance Development Plan (SMDP)	• Draft due within 30 days of contract award • Final due IAW Inspection and Acceptance clause • Updated monthly
5.2.9.4	SW Security Risk Management Plan	20 days after award
5.2.10.6	Test Plans	Per Government Approved PMP
5.2.13.1	Product Configuration Management Plan	30 days after award and
5.2.15	Requirements Traceability Matrix (RTM)	Per Government Approved PMP
5.3.2	Business Requirements Document	Per Government Approved PMP
5.5.2	CAC/PIN Delivery	Per Section 5.5.2 of the PWS
5.5.3	CAC CIF Report	Monthly
5.6.1	Online/Offline Solution	Per government approved Implementation Plan
5.6.9	Update documentation and knowledgebase artifacts	Within 60 days of award, and in conjunction with each release
5.6.10	Remote SW Installation Files	Per government approved Implementation Plan

5.6.11	NTS/ETAS Implementation Plan	Within 30 days of award
5.7.1	ACTUR Project Management Plan	15 days after award
5.7.3.1 5.7.3.5 5.7.3.6	ACTUR Reporting • NCDB Report • NAACCR Report • State Reports • RQRS Service Report • NCDB Data Pull • CCR Data Report • Monthly Activity Report	 Annually Annually Ad-Hoc Monthly Bi-Weekly As Requested Monthly
5.7.3.3	Migrate ACTUR reports from COGNOS to SAS	Per Government approved ACTUR PMP
5.12.1	Implementation Plan	Submitted with proposal and final 15 days after award
5.12.2	Design & implement ACO Demonstration features	In production by November 1, 2019
5.12.3	Update Enrollment Applications	Must be in Production NLT 1 Nov 2019 to support start date of 1 Jan 2020.
5.12.4	New Provider Type	Per Government approved Implementation Plan
5.12.5	Enrollment Fee Wavier	Per Government approved Implementation Plan
5.12.6	PCM Load	Per Government approved Implementation Plan
5.12.7	Implementation of Self Service & Operator Application	Per Government approved Implementation Plan
5.12.8	Letter Modification	Per Government approved Implementation Plan
5.12.9	Develop ACO enrollment, disenrollment, and waiver reports	Per Government approved Implementation Plan
5.12.10	Documentation Updates & Training	Per Government approved Implementation Plan
6.1	Monthly Status Report/Senior Management Review	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.2	Meeting Summaries	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.3	Weekly In-Progress Review (IPR)	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.4	Problem Notification Report (PNR)	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
6.5	Expenditures Resources Report	NLT 25th of each month
6.6	Post Award Orientation	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ

6.7	Final deliverable posted to approved location	Posted no later than deliverable due date
6.8	Quality Control Plan	In accordance with the requirements identified I in the PWS of the EITS II Base IDIQ
8.0	Non-Disclosure Agreement	Prior to any contractor personnel reporting for work
11.3	Tele-work Agreement	Prior to any telework

6.8 Quality Control Plan (QCP)

The Contractor shall follow the QCP requirements identified in the PWS Section 5.9.1 of the EITS II Base IDIQ

6.9 Quality Assurance

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ

7.0 PERFORMANCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

Performance Objective	PWS Paragraph	Performance Threshold	Method of Surveillance
Analysis, design, development and maintenance tasks shall be completed on time in accordance with approved project schedule		Maintain 90% accuracy and timeliness	Periodic (Quarterly)
Work, with limited direction, stays on schedule, on cost, and in scope typically		Meet all government performance, schedule and cost requirements with 95% compliance	Periodic (Monthly)

responsible for independently defining approach to tasks and solutions to problems			
Unscheduled application downtime		Contractor restores application within 48 hours	COR/TPOC monthly review of system metrics
Scheduled application downtime		Equal or fewer than 12 hours	COR/TPOC monthly review of system metrics
Mean Time To Restore (MTTR)		Time allowed for the system to be offline after application availability is interrupted. Mission-critical IT systems (RAPIDS, Application Security, IWS and DEERS) have a MTTR of two hours or fewer; non-mission-critical IT systems (all others) have a MTTR as short as five hours	COR/TPOC monthly review of system metrics
User incidents		(X affected users / Y total users) * 100 = % Application Availability; Maximum % effected dependent on mission criticality	COR/TPOC monthly review of system metrics
Release and Production Drop Schedules		Bugs and defects found in production will not force a rollback 75% of the time	Schedules reviewed at the Weekly IPR
Software Management		98% of scheduled upgrades and/or maintenance are executed according to schedule For non-mission critical applications, 90% of requests for unscheduled software maintenance are responded to within 48 hours For mission critical applications, 100% of requests are responded to within 2 hours	Event Driven and activity reports
Application & System Security Compliance		Maintain 100% application security compliance IAW applicable DoD policy and instruction, DODI 8500.01 – Cybersecurity and DODI 8510.01 - Risk Management Framework (RMF) for DOD Information Technology National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 R4 - Security and Privacy Controls for Federal Information Systems and Organizations DISA - Security Technical Implementation	100% inspection

		Guidelines (STIGS)	
Develop and maintain up-to-date user documentation		100% compliance to Create/Maintain/deliver to government, documentation of all code, to include user help files. Develop and maintain up-to-date digital and hard copy user documentation for framework applications to include user guides, administrator guides, tutorials, and online help within 5 days of release.	Routine Inspection of Deliverable Products/Services
Perform Vulnerability management		Category 1 (CAT I) vulnerabilities eliminated within 24 hours of identification of a vulnerability or the contractor must provide a get well plan approved by the government.	Routine Inspection as Products /Services are submitted
Adherence to Schedule		Contractor meets TO delivery requirements 100% of the time. Unless there is a prior approval from the DMDC COR.	Inspection of Deliverable Products/Services
High Quality Technical Performance *Performance meets all technical and functional requirements, and is highly responsive to changes in technical direction and/or the technical support environment* *Deliverable reports contain all required data and meet all requirements*		Contractor delivery of products and/or services meets all TO requirements. Performance occurs with no required re-work at least 95% of time. Problems that are encountered are minor and resolved in a satisfactory manner.	Routine Inspection of Deliverable Products/Services

8.0 Non-Disclosure Requirements

The Contractor shall follow the Non-Disclosure requirements identified in the PWS Section 8.6 of the EITS II Base IDIQ.

9.0 Cooperation with Other On-Site Contractors

The Contractor shall follow the Cooperation with Other On-Site Contractors requirements identified in the PWS Section 11.7 of the EITS II Base IDIQ.

10.0 KEY PERSONNEL

The contractor shall designate and identify contractor employees who will be considered key to operations for efforts under this task order. These key personnel must have an in-depth understanding of the requirements and their responsibilities as well as the ability, knowledge, experience, and skills to perform the requirements. They shall be fully committed to the success of the mission. The contractor shall designate key personnel for the following tasks:

- Program/Project Manager
- Senior Software Engineer (SSE)
- Information Assurance Manager

11.0 Contract Administration.

This Task Order shall follow all of the requirements identified in the EITS II IDIQ.

11.1 Contract Type: Firm Fixed Price (FFP) and Time and Material (T&M)

11.2 Period of Performance: The period of performance for this Task Order shall be 12 months from date of award with two one year options.

11.3 Place of Performance/Hours of Operation: At least 50% of the work under this task will be performed on site at DMDC facilities in Seaside, CA. The remaining percentage of work may be performed at a contractor provided facility. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section 11.6- Travel. If the contractor anticipates personnel will telework, they shall identify a plan to COR for acceptance.

The contractor is responsible for conducting business between the hours of 8 a.m. to 5p.m depending on their physical location. Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

11.4 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

11.5 Points of Contact:
DMDC COR
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. Ryan Schrank
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: ryan.schrank@gsa.gov
Tel: 215-446-2853

GSA Contract Specialist (CS)
Mr. Mike Levey
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Mike.Levy@gsa.gov
Tel: 215-446-5806

GSA Contracting Officer's Representative (COR)
Mr. Scott Ostrow
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Scott.ostrow@gsa.gov
Tel: 215-446-4497

11.6 Government Furnished Property/Equipment/Information (GFP/GFE/GFI): The Contractor shall follow the requirements identified in the PWS Section 10.8 of the EITS II Base IDIQ.

11.7 Travel: The cost reimbursable not-to-exceed travel limit is estimated at $10,000.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR.
All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.8 Security: The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

12.0 Inspection, Acceptance, and Payment:

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPENDICES

Appendix A – Software Development Roadmap
Appendix B – Automation Standard Best Practices
Appendix C – Enterprise QA Roles and Responsibilities
Appendix D – DMDC ARB Charter References (Enclosure 1)
Appendix E – DMDC ARB Charter Required Artifacts (Enclosure 2)
Appendix F – DMDC ARB Charter Process Map and Description (Enclosure 3)
Appendix G – DMDC ARB Charter
Appendix H – CEAS Project Charter
Appendix I – CEAS Reports List
Appendix J – Template Checklist
Appendix O – EHRM Applications

ITSS Order ID No: 47QFMA18K0030-0013
GSA/FAS Mid-Atlantic Region

Performance Work Statement
Defense Manpower Data Center (DMDC)
Mirador
EITS II Task Order ID03180056012

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) requires information technology services to support technology governance and customer development activities, sustainment and operational activities for the Mirador system across the software development life cycles.

2.0 BACKGROUND

2.1 The Mirador system is designed to meet the Department of Defense (DoD) personnel security mission for Continuous Evaluation (CE) and continuous vetting. Furthermore, Mirador will provide the capability for the DoD to conduct Initial Investigations and Periodic Reinvestigation (PR).

2.2 Mirador is a single DoD enterprise solution, with a data store, interfacing with data providers, and a set of business rules based on the Federal Investigative Standards (FIS), Expandable Focused Investigation (EFI), and Adjudicative Guidelines (AG) for personnel security.

2.3 Executive Order 13467, as amended on September 29, 2016, states that "The Secretary of Defense shall design, develop, deploy, operate, secure, defend, and continuously update and modernize, as necessary, background investigation information technology systems that support all Federal background investigation processes conducted by the National Background Investigations Bureau (NBIB)."

Per a subsequent Memorandum of Agreement between the Office of Personnel Management (OPM) and DoD dated October 3, 2016, DoD has been tasked to "…build, operate, and defend the new National Background Investigation System (NBIS), in accordance with DoD policy and standards. NBIS is an IT system that will satisfy the functional requirements established by the National Background Investigatons Bureau (NBIB) for background investigations." NBIS will be the replacement of the Personnel Security investigation services, currently owned and located in OPM, Federal Investigative Service (FIS). On June 13, 2016, the DoD Chief Information Officer (CIO) tasked the Defense Information System Agency (DISA) as lead for the target/end solution, the NBIS.

A review of the current systems which are owned and operated by the OPM, and a review of current or very near term DoD capabilities were conducted. A determination was made by senior representatives of OPM, Office of Management and Budget (OMB) Performance Accountability Council (PAC), DoD's Office of the Under Secretary of Defense (Intelligence)

(OUSD(I)), DMDC and DISA that DMDC's work with OUSD(I) provided the majority of the capabilities needed to integrate into the end-to-end NBIS. To achieve the current/near term and the final end-to-end solutions for the DoD and Federal enterprise, NBIS requires the services to plan and coordinate the infrastructure, as well as develop, build, and modify applications/systems to be incorporated into the NBIS.

Building and supporting the NBIS requires development and enhancement of multiple applications/systems , to include but not limited to Mirador, Defense Information System for Security (DISS), and Secure Web Fingerprint Transmission (SWFT).

3. SCOPE

The Contractor shall provide the personnel and management necessary to enable the Government to meet the Mirador mission for DoD and ultimately for the Federal enterprise. Services provided under this task order shall include Program Management support, Project Management support, and Software Development Life Cycle (SDLC) requirements. This project will include parallel efforts: 1) the development of a robust Mirador system with the capability of conducting CE checks as well as initial and PRs on the entire DoD population; 2) expansion of the capability to meet Federal populations as serviced by OPM; 3) the integration with other DMDC and non-DMDC systems for the NBIS effort; and 4) the migration, implementation, and sustainment of Mirador within the DISA Defense Enterprise Computing Center (DECC).

4. REQUIREMENTS.

The contractor shall:

4.1 Provide Program Management and Project Management Support

4.1.1 Provide program management support required for a major acquisition program (ACAT 2). Assist the Government in the planning, implementation, and operation of the overall CE/Mirador program development and implementation. Develop and provide an initial program management strategy and plan within 15 business days of Task Order award. Maintain PM strategy and plan and provide weekly status updates.

4.1.2 Coordinate, develop, and document functional requirements with customers and stakeholders. Assist the Government in the documentation of functional requirements. Ensure functional requirements are updated through a Government provided tool or drive within 5 business days of receipt from customers and stakeholders.

4.1.3 Maintain a project management decision log to provide a concise, centralized record for all decisions, approvals and internal and external deliverables. Ensure updates are reflected in the decision log on the Government provided tool or shared drive on a weekly basis.

4.1.4 Review, develop and maintain memoranda and other formal agreements with government and commercial entities to ensure data required to operate the CE Program are obtained and shared legally. Review and coordinate memoranda and agreement with the Government Privacy Office for the development and modification of data provider agreements, Interface Control Documents (ICD), Data Use Agreements (DUA), Memorandums of Understanding or Agreement (MOU/MOA), Concept of Operations (CONOPS), Privacy Impact Assessments (PIA), and other documentation required to operate Mirador and conduct records checks.

4.1.5 Coordinate the development, testing, and refinement of CE business rules with customers and stakeholders. Work with stakeholders to assist with identifying operational processes, supporting cross-organizational agreements

4.1.6 Coordinate, develop, and document ACAT Milestone packages, ensuring that Mirador conforms to systems acquisition policy found in Department of Defense Instruction (DoDI) 5000.02, and complies with information assurance policy in the DoD risk-management framework (DoDI 8510.01) and requirements to manage life-cycle cyber security risks.

4.1.7 Maintain and update the System of Record Notice (SORN) throughout its lifecycle.

4.1.8 Provide monthly status progress reports for monthly status meetings. Include performance metrics identified by the contractor and/or the Government and agreed to by the program management. The meeting dates and times will be designated at kickoff meeting after award.

4.1.9 Continually assess the utility and effectiveness of current and potential data sources to determine whether they are reliable, cost efficient and necessary to meet the requirements of the FIS, EFI, and AG. Provide the assessment results for review at the monthly status meetings.

4.1.10 Serve as a liaison between the data providers, the Government Program and Project Manager(s), and the Mirador development team(s). Regular communication with the Points of Contact (POCs) is required to obtain information regarding upcoming changes in: data formats, data interfaces, new data elements, and new look-up values. Work with the Government leads to standardize the data formats, interfaces and data elements.

4.1.11 Attend and faciliate an estimated 2-5 weekly CE related meetings and workshops. Deliver meeting minutes within 2 business days of the meeting conclusion. Provide meeting summaries that reflect the attendees, meeting highlights, including a list of the issues discussed; any action items created and to whom each is assigned; and all decisions or determinations from the meeting and the decision makers for each. These decisions should be incorporated in the PM decision log.

4.1.12 Provide project management support for the SDLC of Mirador to coincide with the Government process framework for project planning, scheduling, communications, and reporting of all system development activity.

4.1.12.1 Develop a detailed Project Plan Schedule and a technical Implementation Plan that provides the details for the activities associated for the resourcing and scheduling of the Mirador project.

4.1.12.2 The Implementation Plan shall include the proposed steps to complete the integration of Mirador into the NBIS enterprise solution, identifying the resources required, and a schedule for completing the automation and integraton of Mirador in accordance with the NBIS phased development approach. The initial Project Plan Schedule and Technical Implementation Plan shall be delivered 15 business days after date of Task Order (TO) award and shall be updated weekly or as changes occur.

4.1.13 Review, create, and update documentation of the Mirador System as appropriate, to include hardware, software, and web applications along with documentation needed to establish and maintain configuration control of the system throughout its lifecycle. An initial assessment of the status of and need for additional or modified documentation will be delivered within 30 business days of TO award, new documents will be created within 30 business days of notice of the needed document, and updates will be completed within 5 business days of process or application changes.

4.1.14 Deliver functional and technical specifications; such as High Level and Low Level Design Documents and software requirements specification documentation that conform to the Government's software development standards. DMDC's and/or applicable Government software developmet standards are established and available for distribution post award. Ensure that all requirements are documented per standard requirements management processes, base-lined, and tracked to all relevant test and design activities for future use in change control processes. Initial High Level and Low Level Design Documents and software requirements specification documentation shall be delivered within 30 business days of task order award and shall be updated as changes occur.

4.1.15 Identify and track all Mirador system configuration items in accordance with the Government's Configuration Management processes. DMDC and/or applicable Government processes are For Offical Use Only and will be shared post award.

4.1.16 Track and document all software and hardware licenses related to Mirador including expiration dates of licenses throughout the system lifecycle; advise the Government of impending expirations no less than 100 calendar days before the respective expiration dates.

4.1.17 Provide functional and technical expertise to support management of the CE program by analyzing the processes of key program components, support ongoing implementation, enhancements, and changes.

4.1.18 Support customer relationship management interactions with functional, technical, or subject matter level expert services.

4.1.19 Support the management, maintenance, and analysis of data and information. Verify the results of data transfers and data loads.

4.1.20 Assist in developing and delivering materials that are necessary to support the Government's data analysis and IT operations capabilities. Materials that require development and delivery include demonstration web-sites, conference and trade fair participation, meeting attendance and presentations, coordination visits, and supported technology.

4.1.21 Monitor legislative and policy changes; perform regulatory, legislative, policy and standards research and provide assessments of impact to designated programs and IT products; and implement directed legislative and policy changes.

4.1.22 Develop, coordinate, maintain, and update memorandums and other formal agreements relating to research initiatives conducted to improve the efficiency and effectiveness of the Mirador system.

4.1.23 Assist the Government in the development of level of effort assessments, rough orders of magnitude (ROM), and plans of action and milestones for change requests for the Mirador system. Analysis and document coordination shall be completed within 3 business days of change request receipt.

4.1.24 Develop, track and report the technical, programmatic and operational risks and risk handling methods to the program.

4.1.25 Complete ad hoc reporting requests within 10 business days. Examples of ad hoc reporting requests include numbers of personnel by component enrolled in Continuous Evaluation, numbers of alerts generated by data source type, etc.

4.1.26 Resolve identified data quality issues within 10 business days. Resolution of data quality issues will be demonstrated through queries of data in the system by the Government or the contractor to demonstrate that identified problems have been remediated.

4.2 Support the Development of the Mirador System

Support and complete the development of the Mirador system:

- Integration - Provide Software Maintenance and Sustainment of Mirador. Integrate Mirador into NBIS in accordance with the approach required to integrate multiple new and operational capabilities into an end-to-end solution to replace legacy systems operational capacity.

- Automation - Develop the full enterprise system capability by interfacing Mirador with other DMDC, DoD, Federal, State, and local government and criminal justice agency systems, and commercial systems required to conduct Initial and PRs. Automate Mirador's reporting capability for Initial/PR reports and CE alerts and complete baseline requirements in support of the NBIS.

- Additional Development - Develop Government requirements for Mirador to sustain Full Operational Capability (FOC) ensuring the system has met all technical, functional, and user requirements defined by the sponsor to include all available data sources implemented in the enterprise solution for CE and Initial and PR capability.

4.2.1 Develop, implement and test the latest FIS, EFI, AG rules, or Security Executive Agent Directives (SEADs) to generate alerts that are sent for validation and adjudication.

4.2.2 Evaluate CE processes, procedures, data and business rules to provide recommendations for improvements to the efficiency and effectiveness of the DoD CE Program. An evaluation update will be provided in the monthly meeting.

4.2.3 Ensure the operation of Mirador is in accordance with the System of Records Notice (SORN).

4.2.4 Evaluate, incorporate, and test additional data sources that meet the data categories of the Director of National Intelligence's (DNI) CE Program: clearance, credit, terrorism, foreign travel, suspicious financial activity, criminal activity, and commercial data sources. This includes the implementation of business rules specific to the data sources.

4.2.5 Develop and implement expanded use of Mirador for a broader continuous evaluation population up to and including all Federal government agencies.

4.2.6 Develop and implement a solution that will have the capability of supporting traditional Initial Investigations and PRs as defined in the FIS, as directed by the Security Executive Agent (SecEA), or as directed by the Executive Office of the President.

4.2.7 Sustain the Mirador application in the the DISA Defense Enterprise Computing Center (DECC) environment as coordinated by the Government. Support includes assisting the Government with fully documenting the necessary steps, activities, milestones, timelines, and risks.

4.2.8 Implement CE Working Group (CEWG), and other stakeholder requirements based upon prioritization by the Government. Support includes additional or updates to automation, workflow, graphical user interface (GUI), and user roles.

4.2.9 Support customer specific and system reporting metric capability. This includes the creation of scripts and/or web-based reports as determined by the Government. The reporting requirements will change as the system is migrated to NBIS. The contractor shall propose system metrics which will be reported on a regular basis for the Government to measure the efficiency and effectiveness of the system. (Proposed metrics shall be delivered within 180 calendar days of contract award).

4.2.10 Verify documents (such ICD and data agreements) are current and in place prior to connecting to any data provider and external system. This also includes confirming the data providers and/or external systems have the DoD approved certificate prior to establishing system connectivity with Mirador. The artifacts shall be maintained by the contractor as identified in PWS sections 4.1.2, 4.1.3, and 4.1.4.

4.2.11 Complete quality assurance testing to ensure that the system modifications meet the functional and user requirements. This includes performing the necessary operational, functional, regression and user acceptance tests, and resolving any internal or external issues to include technical issues with data providers.

4.2.11.1 Produce functional test guides

4.2.11.2 Implement and update the Mirador Master System Test and Evaluation Plans.

4.2.12 Deploy the software code to Mirador's production environment, produce release notes, and ensure that the modifications meet the requirement during the production data run.

4.2.13 Support the development of the Mirador System Security Plan (SSP) and attaining and/or maintaining of the Authority to Operate (ATO). Ensure that Mirador continually complies with all Security Technical Implementation Guides (STIGs) and information assurance (IA) guidelines.

4.2.14 Maintain a project management decision log to provide a concise, centralized record for all decisions, approvals and internal and external deliverables.

4.2.15 Verify the results of data transfers and data loads. Take corrective action when errors occur and document log errors and corrective action.

4.2.16 Establish and maintain system interfaces, secure file transfer capabilities, conduct necessary checks, and provide reports defined in the CONOPS.

4.2.17 Comply with all relevant policies, procedures, agreements and contracts associated with CE data providers.

4.2.18 Comply with Government standards for common builds and Configuration Management (CM) processes as specified by the Application Development Process. This includes versioning application code for each deployment, building deployment packages, developing (and implementing, if required) back-out plans, recording and reporting the status of the deployed applications, and verifying the completeness and correctness of the deployed applications.

4.2.19 Review existing Configuration Management (CM) documentation for Mirador and ensure that it remains current. Provide edits to CM process flows, CM training documents, and CM infrastructure diagrams within 5 business days of system changes. Manage and process all Mirador system configuration items in accordance with the Government Configuration Management processes.

4.2.20 Maintain data modules for each data provider and the ICDs. As changes occur, maintain versions and formats, data elements in the interface and tables, look-up values, and data transfer methods, such as web services.

4.2.21 Support Emergency Maintenance events. In the event of unscheduled application outages perform diagnostic testing to identify root cause(s) for the application outage; develop necessary application remediation plan(s); and apply emergency fixes.

4.2.22 Perform remediation of security vulnerabilities and take immediate action to assess the impact, develop patching plans, provide First Report requirement, create the necessary Plan of Action and Milestones (POA&M), and test patches to ensure the patches create no negative impact to the systems. Testing shall be conducted to ensure Information Assurance Vulnerability Management (IAVM) actions will not impair system operations. Coordinate with Government Cybersecurity team on system security matters, address specific security issues, and obtain guidance.

4.2.23 Develop, maintain and update system documentation as required. A particular type of documentation needs to be delivered with a software release only if/when an update is required.
The list may include but is not limited to:

- Software Requirements Specification
- Software Project Management Plans
- Process and product documentation
- Architecture/Design Documentation
- Technical, user, and system documentation
- System Administration and Installation Guides
- Data Models

- Data Dictionaries
- Interface Documentation
- COOP Plans
- Deployment Plans
- Requirements Traceability Matrix
- Configuration Management Plan
- Test and Evaluation Plans
- Data Quality Reports/Plans
- Reporting Requirements Plans
- Use Cases
- Information Assurance Reports
- System Backup/Recovery Plan
- Coding Standards Guide
- Software Quality Plan
- System Security Plan

4.3 Conduct Risk Management Framework (RMF) Assessment and Authorization Process Support

Assist the Government's Cybersecurity and Information Technology teams with the Risk Management Framework (RMF) Assessment and Authorization Process in order to sustain ATO and maintain the security posture of the CE systems, as outlined in DoD 8510.01. Common types of deliverables for this task include Account Management guides, Concepts of Operations, POAMs, answers to interview questions, audit logs, scan results, etc.

4.4 Implement Program Enhancements in support of NBIS (Time & Materials – NTE $5M)

4.4.1 Assist the Government in the implementation of the Mirador program from a DoD-only program to implantation across several Federal agencies. Support the expansion of infrastructure, move to the DISA DECC and/or Cloud envvironment, provide system development support and future modifications, testing and production environments, addition of data interfaces with various Federal systems, and management of Federal users and subjects.

4.4.2 Support the integration of Mirador with other applicable systems (e.g. DISS) to support a common NBIS Data Repository that will be shared with other NBIS systems. This may require modifications to the applications to include new functionality as well as the modifying the underlying architecture.

4.4.3 Integration of the systems may highlight areas where the applications can be standardized and data rationalized for efficiencies. As assessment and integration work is done, the contractor will identify those areas that can be standardized and data can be rationalized to improve integration with other applicable NBIS systems and achieve the NBIS phased vision/goal.

4.4.4 As the requirements for modifications of the systems are identified, the contractor will propose methods to increase the security of the overall system to include modification of security controls and postures of Mirador to include the architecture, data, and application layers.

4.4.5 In coordination with DISA, implement the processes as identified in the Business Process Re-engineering efforts conducted by DoD and NBIB for the Federal Security, Suitability and Credentialing processes.

4.4.6 Design, develop, and test new application requirements as determined by the NBIS Information Technology Governance Board (ITGB).

4.4.7 Support full scale testing of the applications by the Joint Interoperability Test Command (JITC) or other designated tester, and make any required application changes in response to deficiencies found during testing.

4.4.8 Create and maintain appropriate system and process documentation for establishment and operation of Mirador as part of the NBIS effort.

4.4.9 Provide for data processing of externally provided files until an automated interface and workflow is implemented within the system.

4.5 Quality Assurance

4.5.1 Provide Quality Assurance Support in accordance with established processes and procedures. Define and develop test plans, test scripts, test cases; track and report issues; conduct testing and measure the success during and after testing; and evaluate and document test results. Conduct Quality Assurance (QA) projects, using documented requirements provided in functional, technical or application release scope specifications. Provide QA support, which includes releases for: Shared libraries, single table updates, web applications, web services, applications, reports, modules, software programs, etc.

> 4.5.1.1. The Government estimates 12 releases per 12 month period of performance (1 major and 3 minor releases quarterly). Any given release shall be comprised of any or all MIRADOR system components. A major release is a deployment of new application functionality and a minor release is maintenance-related.

4.5.2 Quality Control Plan (QCP)

4.5.2.1 The Contractor shall follow the QCP requirements identified in the PWS Section 5.9.1 of the EITS II Base IDIQ.

4.5.3 Risk Management Plan (RMP)

4.5.3.1 Assess, evaluate, document, and manage risks associated with the performance of this task order. Create, modify, maintain, implement and deliver a task order specific Risk Management Plan within 30 calendar days of Task Order award.

4.5.4 Work Breakdown Structure (WBS)

4.5.4.1 Submit a Work Breakdown Structure (WBS) within 30 calendar days of Task Order award. This WBS shall detail the decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables in accordance with the statement of work and the requirements levied against the program.

4.5.4.2 The WBS shall define each of the tasks required to complete the work, identify individual responsibilities, and describe output, timelines for completion and performance standards. The WBS shall identify final completion dates and progress milestones for tasks and provides a basis for monitoring and evaluation contractor work.

4.5.4.3 The WBS may be changed due to changing requirements/requests from the functional sponsors. If that occurs, the contractor will provide the impact to the original WBS (to include dependencies for the critical path), and schedule and resource modifications to be made with the new approach. These items will be delivered within 5 business days of the proposed change and also discussed at the monthly status meeting.

4.5.4.4 The Contractor shall maintain a Lessons Learned document, updating it subsequent to each software release, disseminate and make recommendations to the Government to increase the quality of future deliverables and improve reliability and efficiency of systems.

4.5.5 Participate in Kick Off Meeting

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the contract and will aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements at the time offers were submitted nor is it to be used to alter the final agreement arrived at in any negotiations leading to contract award. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the COR. The meeting will take place within 14 business days of Task Order award. Kick off meeting minutes are due to the COR within 5 business days of the kick off meeting.

4.6 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.7 CONDUCT ARCHITECTURAL ANALYSIS

4.7.1 Define and document as-is and to-be architecture environments.

Maintain As-Is artifacts provided by the Government for the life-time of the contract.

4.7.1.1 All recommendations shall be submitted in the form of to-be documentation to the Government within 30 days.

4.7.1.2 All as-is and to-be artifacts shall include:

- Project Charter
- Project Plan (Timeline)
- "DoDAF" hybridized systems view
- SV-1*Future Requirement
- Application Security Plan and PII Checklist
- Application Support Plan
- Functional Specification
- Technical Spceficiation
- Requirements Traceability Matrix (RTM)
- Configuration Management System Request for Change (CMS RFC)
- Application and Data Asset List Information
- Data Model

4.7.2 Provide current state application modeling support

4.7.2.1 Create current state application modeling in coordination with Architcture Review Board (ARB) and other entities as part of the modeling efforts, maintenance of system inventories, integration with Government service management processes, configuration management and change impact analysis and reporting on application deployment.

4.7.2.2 Document and maintain current state application inventory, deployment details and information to enable configuration management. Documentation shall be created using the Government standardized Enterprise Architecture Repository, include full system and asset inventory, and provide reporting capabilities at the request of the Government.

4.7.2.3 Support the Government Architecture Program Manager responsible for the definition, documentation, and execution of the Government EA business structure and the Software Development Life Cycle (SDLC) process, its policies, processes and standards. See enclosure ARB Process Map and Description Enclosure for process steps.

4.7.2.4 Support architectural and technical oversight engagement activities including long and short term participation with application development and IT infrastructure operations teams providing full SDLC support, tool support, mentoring, and architectural design and implementation support with consideration for application performance.

4.7.2.5 Identify, document, track and execute risk mitigation strategies that address the Government exposure in the development, integration, deliverables, and deployment efforts for all collaboration efforts with external and internal stakeholders. Initial Risk Mitigation Strategeis shall be delivered within 45 calendar days of Task Order Award; tracking and maintenance of this document shall occur bi-weekly.

4.7.3 Assist the CIO Office with the planning, design, configuration, and establishment of application in the NBIS or defined Government infrastructure and architecture. Develop recommendations for the integration of Mirador.

4.7.3.1 Incorporate and/or revise technical architecture components, to include modifications necessary for the NBIS effort.

4.7.4 Provide Architectural Support

4.7.4.1 Conduct architecture analysis to analyze existing architectural structure. Document analysis findings and submit to the Government within 135 days of TO award.

4.7.4.2 Work with the architecture team on TO 3 to ensure data modeling and diagrams are kept current and updated in the current approved system.

4.7.5 Assist the CIO Office with the planning, design, configuration, and transition support for Mirador into the NBIS infrastructure and architecture. Support will require coordination and collaboration with other Federal Agencies (i.e. SPAWAR) integration into the NBIS environment. Provide detailed artifacts needed for full transition and integration of Mirador into the DISA Defense Enterprise Computing Center (DECC) as part of the NBIS effort.

4.7.6 Provide Architecture Sustainment Support

4.7.6.1 Research new techniques and standards from the government and industry to implement best practices, refine knowledge, and provide guidance through assisting or providing formal and informal knowledge transfer to Government staff.

4.7.6.2 Support Architecture maturation efforts by assisting in the identification and documentation of recommendations for process improvements, new process adoption efforts, and tool adoption and support. Identification and documentation of issues and

recommended resolution support includes tasks such as process mapping, point papers, process research and reengineering, and implementation support, etc., for Government approval and implementation.

4.7.6.3 Provide business architecture documentation support that provides information for decision making for the Government regarding effective IT investments supporting business requirements.

4.7.6.4 Work with Government team(s) to complete business and IT architecture planning.

4.7.6.5 Develop for Government review and approval, IT vision and business/IT alignment statements.

4.7.6.6 Establish and document the alignment of business, functional, and IT goals and objectives.

4.7.6.7 Conduct analysis support to ensure requirements compliance, identify problems, correctly attribute them to automated processes and/or submission data and develop solutions.

4.7.6.8 Respond to ad hoc research requests from management to include: performing special studies, conducting data research and respond to inquiries for customers.

4.7.6.9 Develop and maintain architectural design documents and present to the Government for review and approval.

4.7.6.10 Support the development and maintenance of comprehensive Data Management Programs that include key components such as data architecture; data dictionary; data models; data and metadata repositories; data stewardship; data quality; data acquisition; data usage; and data retention. Initial Data Management Plans are due 45 days after TO award; plans shall be updated as requires and newly created documents shall be delivered within 30 days of requirement/acknoweledgement.

4.7.6.11 Work with Government team(s) and provide assistance in supporting the development of data architecture planning and implementation initiatives.

4.7.6.12 Determine project schema requirements and establish guidance on enterprise modeling standards as they apply to the production and test databases.

4.7.6.13 Participate in logical database design and modeling. Collaborate with the data architects and the enterprise data modeler team to review and publish application logical data models.

4.7.6.14 Make recommendations for incorporating NBIS approved technical architecture components into application using approved software frameworks (e.g. J2EE, Common Update Framework (CUF) and Application Security).

4.7.6. Conduct application architecture initiatives, such as, identifying and classifying application components according to the specific business and performance objectives they support and the technologies they employ.

4.7.6.16 Document and perform analyses of the current application inventory and provide detailed application architecture guidelines to improve both business and technology processes and applications in the interest of integration and cost containment. Application analysis may require research of interoperability capability, performance and scalability, reliability and availability, application lifecycle stage, and technological risks.

4.7.6.17 Provide support to identify and recommend application delivery; what technologies should be used to deliver them, and how the applications should be designed, deployed and integrated in the most effective and flexible way.

4.7.6.18 Recommend updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments with impact analysis for Government review and approval.

4.7.6.19 Support requirements gathering and high-level design for IT application development.

4.7.6.20 Support development of business requirements documents.

4.7.6.21 Assess and document the alignment of applications/services to Agency programs.

4.7.6.22 Work with Government team(s) to support application architecture planning, implementation, and maintenance.

4.7.6.23 Provide support in assessing performance of applications in producing business value and return on investment.

4.7.6.24 Work with Government team(s) to support IT architecture/infrastructure planning, implementation, and maintenance.

4.7.6.25Provide technology assessment evaluations as required.

4.7.6.26 Identify and document hardware and software technology refresh recommendations.

4.7.6.27 Evaluate opportunities for delivery of common capabilities for describing, organizing, integrating, sharing and governing information assets.

4.7.6.28 Prepare application & infrastructure for migration to Defense Information Systems Agency (DISA) data center.

4.7.6.29 Provide support in assessing performance of infrastructure in producing business value and return on investment.

4.7.6.30 Input all modeling artifacts into the Government defined system.

4.8 Defense Vetting Enterprise (OPTIONAL)

4.8.1 The Defense Information Systems Agency's (DISA) National Background Investigation Service (NBIS) will soon fall under the authority, direction, and control of the Director of Defense Security Service (DSS), according to a memorandum issued by the DEPSECDEF Memo, dated 28 Jan 2019, for Transfer of Functions to the DSS to support the Defense Vetting Enterprise.

The memorandum directs the move of the NBIS Program Executive Office and subordinate elements, the Department of Defense Consolidated Adjudications Facility (DOD CAF), as well as Joint Service Provider (JSP) personnel providing direct support to the DOD CAF. This realignment further strengthens the department's personnel vetting enterprise and supports the transfer of DOD CAF functions, personnel, and associated resources to the DSS, which was mandated by Subsection 925(c) of the National Defense Authorization Act for fiscal year (FY) 2018.

In 2016, DISA was tasked to design, develop, test, field, operate, maintain, and secure an information technology system, or suite, to conduct background investigations for civilian employees, military service members, and government contractors. Since then, DISA has led the effort in collaboration with the Office of Personnel Management National Background Investigations Bureau, the Defense Manpower Data Center, and other DOD agencies.

This request is driven by DSS request for a single interface to consume data elements from DMDC's data catalog as they transition the Secure Web Fingerprint Transmission (SWFT), Defense Information System for Security (DISS) and MIRADOR outside DMDC boundaries. DMDC is responsible for migrating the data from JPAS to the DISS data stores (Joint Verification System (JVS), Information Delivery System (IDS), and the Case Adjudication Tracking System (CATS).

4.8.2 The objective is to evaluate existing DMDC mechanisms for data delivery including, Real Time Broker Service (RBS), Batch Broker Service (BBS), ARROW, manual data requests and individual web services and propose a solution to consolidate multiple data streams into an enterprise solution, allow for the incorporation of additional data sharing capabilities and expand data holdings available to include Person Data Repository (PDR), other DMDC data holdings, and external datasets.

4.8.3 *The Contractor shall provide support for the tasks described below:*

4.8.3.1 DEVELOP A DATA DELIVERY WEB SERVICE

4.8.3.1.1 Provide a Project Management Plan (PMP) that describes milestones, tasks, and subtasks required in this call. The PMP shall identify and assign tasks, major milestones, dates, dependencies and indications of critical path. The PMP shall include the status; statistics; risk management review; critical path; and other milestone progress checks and updates; as well as a project schedule. Tasks from the final and Government approved PMP shall be selected as milestones against which Contractor's progress will be monitored. The PMP is an evolutionary document that shall be updated annually and identify tasks and deliverables specified in Service Delivery Roadmap. Any updates to the PMP will be incorporated to the Call Order upon Government approval and updated weekly in project server.

4.8.3.1.2 Coordinate with all DMDC governance bodies for approvals is mandatory and will be in accordance with DMDC prescribed Business Process and subsequent updates. These groups include, but not limited to, the Requirements Review Board (RRB), Architecture Review Board (ARB), Change Advisory Board (CAB), Executive Governance Council (EGC), Enterprise Quality Assurance (QA), DMDC Management Advisory Group (DMAG), Cyber Hardening Working Group (CHWG) and all impacted divisions for project requirements, dependencies and execution for approval authority. The Contractor shall satisfy Information Assurance (IA) requirements to include developing artifacts IAW DoD Instruction 8510.01 (RMF for DoD IT) and supporting the Government in obtaining an Authorization to Operate (ATO). Adhere to all DMDC Business Process Re-Engineering (BPR) workflows, requirements, and tool usage.

4.8.3.1.3 Perform requirements management to include gathering requirements and creating and maintaining requirements traceability (RTM). Document functional and technical requirements, create analysis and design documentation, program specifications and unit test criteria. Provide the following documents:

- Software Requirements Specification (SRS)
- Concept of Operations (CONOPS)
- Interface Control Document (ICD)

- Requirements Traceability Matrix (RTM)

4.8.3.1.4 Define the to-be architecture, conduct a design review and document the architecture design in SPARX.

4.8.3.1.5 Create a data delivery web service that delivers data leveraging a pre-defined list of interfaces (DISS, MIRADOR, and SWFT) and based on business requirements, to-be architecture, and design. The solution must:

4.8.3.1.5.1 Provide a single enterprise connection (or minimum) number of separate interfaces for a given customer to be able to connect to DMDC to obtain a wide set of data attributes

4.8.3.1.5.2 Contain a HTTPS enabled interface

4.8.3.1.5.3 Accessible externally

4.8.3.1.5.4 Batch capabilities

4.8.3.1.5.5 Accessibility thru CUF

4.8.3.1.5.6 Query response

4.8.3.1.5.7 Scalable and secured solution

4.8.3.1.5.8 Capable of providing 99.9%data availability per year

4.8.3.1.5.9 Ingested automatically without human intervention (Fully automated)

4.8.3.1.6 Perform software testing as the software is being developed; document the primary testing methods, and test cases used. Quality Assurance (QA) testing for all releases are conducted by DMDC's Enterprise QA team. Enterprise QA performs software testing and performs the following duties: define and develop test plans, test scripts, test cases; track and report issues; conduct testing and measure the success during and after testing; and evaluate and document test results. The Contractor shall support Enterprise QA and provide the following artifacts:

- Requirements Traceability Matrix (in order for QA to map requirements to test cases)
- Functional Specifications
- Release notes (states summary of functionality/ additions/ modifications made to application)
- Resource Request form (this is an enterprise QA provided form that is completed at least four (4) weeks in advance of QA resource request

4.8.4 Submit Reports & Documentation

The contractor shall provide initial draft(s) of and update Government recommendations, for Government approval, as changes in processes and procedures occur.

4.8.7 Conduct Bi-Weekly In-Progress Reviews (IPR)

Conduct a bi-weekly IPR to discuss program, project and service status, existing or potential problems, and projected tasks and milestones. In addition, the contractor shall provide updates to the PMP at the IPR. The contractor shall participate, document, and distribute minutes of regularly scheduled weekly status report meetings. The contractor shall meet with the Government Program Manager to discuss technical matters, share ideas, review milestones, activities accomplished, new and current issues and work progress. In addition, discuss and work out any outstanding administrative or managerial issues.

4.8.8 DELIVERABLES/PERIOD OF PERFORMANCE

The maximum duration of the project is five (5) months from the date of award, as per the following deliverables:

PWS #	PWS Section	Date Due/Frequency
4.8.3.1.1	Project Management Plan & Schedule	Draft submitted ten (10) days of award; Final submitted within ten (10) days after receipt of Government comments. Updates as needed, and no less frequently than 5 days after exercise of an Option Period.
4.8.3.1.2	Documented DMDC Governance approvals	Per Government approved project plan
4.8.3.1.4	(1) Software Requirement Specification (SRS) (2)CONOPS (3) Interface Control Document (ICD)	25 days after award
4.8.3.1.4	Architecture Design	30 days after award and updated monthly
4.8.3.1.5	DSS Data Delivery Solution	30 Nov 19
4.8.3.1.6	Requirements Traceability Matrix (RTM)	Draft – at each release Final – at beginning of Enterprise QA testing
4.8.3.1.6	QA Test Artifacts ➢ Functional Specification ➢ Requirements Traceability Matrix (RTM) ➢ Release Notes ➢ Resource Request Form	4 weeks in advance of QA resource request

	IAVM Remediation	Within the timeframe stipulated by DMDC Cybersecurity Branch.
4.8.5	Monthly Status Report (MSR)	MSR shall be conducted on the 15th working day of each month; electronic copy of brief shall be delivered 3 days prior to the brief.
4.8.6	Problem Notification Report	3 days after identification of problem
4.8.7	Weekly IPR	Weekly - Written report is due 1 day prior to meeting
	Post Award Conference	Within 5 days of award

5.0 QUALITY SURVEILLANCE

5.1 The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

5.3 Customer Complaint Surveillance.

This action is instituted when the PM, GSA COR receives a complaint from a stakeholder (stakeholder organizations include P&R IM, DPRIS User Agencies, Military Service Repository Owners, and the Defense Information Systems Agency) regarding contractor service. The PM will obtain the complaint in writing and then conduct an investigation to determine its validity. If the complaint is deemed valid, the PM will immediately notify the GSA Contracting Officer for action. The PM will notify both the Contract Manager and the complainant of the Government's response to their complaint.

5.4 Contract Discrepancy Report (CDR).

In the event of unsatisfactory contractor performance, the COR will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The

contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

5.5 Problem Notification Reports (PNR).

The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ.

5.6

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	Contractor shall submit to the COR for review and approval. The COR shall maintain a log on submitted deliverables and corrections required.
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) business days.	The log will identify the timetable and schedule for on time submission
Business Relations: Proactive in identifying problems and	Clear and consistent written or verbal communication, responses and/or acknowledgement within	The log will identify the problems and recommended solutions;

recommending implementable solutions	one (1) working day of identifying events that required decisions or actions by program management or being contacted by the government.	email verification, visual inspection
Key Personnel: Provide qualified personnel in a timely manner.	New or replacement personnel in place within five (5) business days of negotiated date.	Contractor shall submit via email or in writing to the COR notification when replacement personnel are in place.
QA Specific Objectives		
Provide the percentage of test case execution. Unless otherwise agreed upon with the government project manager, test case execution must be 100% for all projects. Provide on the signoff documentation to project teams.	% of test case execution (indicates the progress of testing by giving the percentage of test cases executed with the result of a pass, fail, or blocked result) Percent of Test Case Execution = (Number of Passed Tests + Number of Failed Tests + Number of Blocked Tests) / Number of Test Cases	The log will identify the QA metrics; visual inspection of test results.
Provide the defect removal efficiency. DRE must remain >95%. Report progress in MSR.	Defect Removal Efficiency (No. of Defects found during QA testing / (No. of Defects found during QA testing +No. of Defects found by End user))	The log will identify the QA metrics; visual inspection of metrics
Provide defect leakage rate. Rate must remain at 5% or less. Report progress in MSR.	Defect Leakage (used to identify the efficiency of the QA testing) = (No. of Defects found in UAT / No. of Defects found in QA testing) * 100	Visual inspection of monthly status report
Maintain automated test cases. Report progress in monthly status review.	Maintain 95 - 100% automated test cases.	Visual inspection of monthly status report
Reduce PII in historical test case data. Report progress. Report progress at Monthly Status Report	Remove identified cases and provide reporting each month.	Visual inspection of monthly status report
Respond to all calls related to incidents affecting production within fifteen minutes, in the event that the incident requires QA to	Respond to 95% of all calls within 15 minutes.	Visual inspection of monthly status report

test a behavior in production. Report progress in MSR.		

5.8 Acceptance of Documentation

Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, shall be applied to each deliverable received from the contractor under this task order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow Government guidance. Where none exists, the contractor shall coordinate approval of format with the PM.
- Timeliness – Deliverables shall be submitted on or before the due date specified

6.0 DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within 10 business days from Government receipt of the draft deliverable using the Deliverable Acceptance Checklist.

Deliverable	PWS Reference	Delivery Date
Program Management Strategy and Plan	4.1.1	Initial due 15 business days after TO award. Status updates due weekly.
Functional Requirement Documentation	4.1.2. 4.2.11	Within 5 business days of receipt or collection of requirements from customers and stakeholders; as required
Project Management Decision Logs	4.1.3, 4.1.11, 4.2.14	Weekly
Results of Reviews of Status of Time Sensitive Documentation	4.1.4	Monthly

New or modified business rules	4.1.5	As required
ACAT MS packages	4.1.6	5 business days prior to each MS and major decision point
Maintain, Update, and Adhere to SORN	4.1.7, 4.2.3	As required
Progress and Performance Meeting and Reports	4.1.8	Monthly
Data Source Assessments	4.1.9	Monthly
Status of Data Format, Interfaces, and Data elements Standardization	4.1.10, 4.2.16, 4.4.3	Monthly
Meeting Minutes	4.1.11	Within 2 business days of meeting
Project Plan Schedule	4.1.12.1	Initial due 15 business days after TO award. Updated as changes require.
Implementation Plan	4.1.12.2	Initial due 15 business days after TO award. Updated as changes require.
Documentation of the Mirador System	4.1.13, 4.2.23	Initial due 30 business days after TO award. Updated as changes require. Newly created docs within 30 days.
Functional and Technical Software Specifications	4.1.14	Initial due 30 business days after TO award. Updated as changes require. Newly created docs within 30 days.
Configuration Management Documentation	4.1.15, 4.2.18, 4.2.19	As changes occur, but within 5 business days of system changes
Status Report on Software and Hardware Licenses	4.1.16	Monthly
Support Functional and Technical expertise	4.1.17, 4.1.18, 4.1.19	As required
Web-site Demonstrations, On-site System Demonstrations, Meeting Presentations	4.1.20	As required
Legislative, Policy, and Standards Changes Findings	4.1.21, 4.2.18	Monthly
Interagency and support agreements	4.1.22	As required
Level of Effort Assessments, ROMs, and Plans of Action and Milestones for Change Requests	4.1.23	Within 3 business days of receipt of change requests

Report of Technical, Programmatic, and Operational Risks and Risk Handling Methods	4.1.24	Monthly
Ad Hoc Reporting	4.1.25	With 10 business days of reporting request
Resolution of Data Quality Issues	4.1.26	With 10 business days of receipt of issue
Software Modifications to Align Mirador with Federal Requirements	4.2.1,	As required
Recommendations for Process Improvements	4.2.2	Monthly
Application code for new populations, data sources, and associated business rules	4.2.4, 4.2.5, 4.2.6	As required
DISA DECC Migration/Sustainment Documents	4.2.7	Within 30 business days of receipt of requirement
Proposed Performance Metrics	4.2.9	Within 180 calendar days of contract award.
Functional Test Guide	4.2.11.1	Due 15 business days prior to scheduled testing.
Master STEP	4.2.11.2	As required
Release Notes	4.2.12	Due 15 business days from software deployment
Mirador System Security Plan revisions	4.2.13	As changes occur
Log Errors Documentation	4.2.15	Within 3 business days of errors in data transfers and data loads
Data Module Updates	4.2.20	As changes occur
Emergency Maintenance	4.2.21	As required
POA&Ms and Test Patches for Security Vulnerabilities	4.2.22	As required
Risk Management Framework Assessment	4.3	As required
Implement Processes identified by DoD and NBIB in Support of NBIS	4.4.1, 4.4.5	As required
Integration of Mirador SWFT DISS and/or NBIS	4.4.2	As required
Recommendations for Methods to Increase Security of Mirador	4.4.4	Address in monthly status reviews
New Application Requirements	4.4.6	As required

Support JITC Testing	4.4.7	As required
System and process documentation for Mirador as part of the NBIS effort	4.4.8	As changes occur
Quality Management Plan	4.5.1	Updated upon request by government.
QA Metrics	4.5.1	Within 7 days of QA support begin date, or upon request by government.
QA SharePoint site maintenance	4.5.1	Weekly or upon request by government.
QA Testing Strategy	4.5.1	Updated upon request by government.
Staffing Plan		Within 10 business days of award.
Automated Test Scripts	4.5.1	Within 7 business days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Test Case Report	4.5.1	Monthly with MSR reporting
QA Test Plans	4.5.1	Within 7 business days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Level of Effort and Resource Estimate	4.5.1	Initial estimate provided within 2 business days of project notification; final provided within 7 business days of project finalization notification.
Requirements Traceability Matrix (RTM)	4.5.1	Updated within 7 business days of government notification requesting initial QA support. Weekly for ongoing iterations, or upon request by government.
Testing Results and Change Management System (CMS) Region level readiness	4.5.1	7 business days prior to release to planned production or contractor test environment.
Issue Tracking Tickets and Reporting	4.5.1	Issues logged within 24 hours of discovery and reports
508 Compliance Audit Report	4.5.1	Quarterly; provide report within 7 business days of concluded audit.
QA In Progress Review (IPR) Agenda	4.5.1	Weekly.
QA IPR Meeting Minutes	4.5.1	Within 48 hours of IPR meeting

QA Off Hours Reporting	4.5.1	Weekly.
Functional and Technical Meetings	4.5.1	Weekly/Monthly/Ad Hoc.
Quality Control Plan	4.5.2	Initial due 30 business days after TO award. Updated as changes require.
Risk Management Plan	4.5.3	Initial due 30 business days after TO award. Updated as changes require.
Work Breakdown Structure	4.5.4	Initial due 30 business days after TO award. Updated as changes require.
Lessons learned Document	4.5.4.4	Within 15 business days of SW release
Kick off Meeting	4.5.5	Within 14 business business days of TO award
Kick off Meeting Minutes	4.5.5	5 business days of kick off meeting
SMR	4.6	NLT 10th of each month
Update or revise technical architecture designs and components	4.7.2	As needed
Risk Mitigation Strategies	4.7.2.5	Within 45 days of TO award, and update as required
Architecture Analysis	4.7.4	As needed
Develop plans, artifacts and design configurations in Government infrastructure	4.7.5	As needed
Develop and montain Data Management Plans	4.7.6.10	Initial due within 45 days of TO award. Updated as changes required. Newly created docs within 30 days.
Data Architecture planning	4.7.6.11	As required
Database design and modeling	4.7.6.13	As required
Document and perform analyses of the current application inventory	4.7.6.16	As required
Technology Assessment evaluation	4.7.6.25	As required

7.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets,

copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

The Government will provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; commercial off-the-shelf software; hosting facilities; and all other relevant materials and equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support. All Mirador documentation, code, data, and other materials generated or received in the course of contract performance remain the property of the U.S. Government.

8.0 PLACE OF PERFORMANCE / HOURS OF OPERATION

8.1 The work under this task shall be performed primarily on site at DMDC facilities in Seaside, CA or Alexandria, VA. Work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section 10.0- Travel.

8.2 The contractor is responsible for conducting business between the hours of 8 a.m. to 8 p.m. ET, Monday thru Friday except Federal holidays. The contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

8.3 The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following:

- Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.
- Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment

9.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order will be one 6-month base period and four 3-month options.

10.0 TRAVEL

10.1 The Government anticipates some travel between Seaside, California and the National Capitol Region(estimated at approximately 2 personnel per quarter). Should travel be required, the following applies.

10.2 Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. All travel shall be coordinated in writing through the PM or COR and travel must be pre-approved by the GSA CO (or their designated representative) prior to incurring costs..

10.3 All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

10.4 Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government, not to exceed **$30,000.00 for the Base and Option Years**. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

10.5 Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel. The Contractor shall make every effort to travel as efficiently as possible. Air travel shall be accomplished on regularly scheduled commercial flights using the most economical manner consistent with the successful accomplishment of the work. Reimbursement of lodging and incidental expenses shall be limited to the government per diem rates as stated in the Joint Travel Regulations (JTR) and FAR Part 31.205-36 (Travel Costs). Travel costs shall be reimbursed to the Contractor only to the extent that it is necessary and authorized for performance of the services under this task order. Reimbursement for the costs of subsistence and lodging shall be considered to be reasonable and allowable daily charges as compared to the maximum rates set forth in the following:

a. Joint Travel Regulations Volume 2, DOD Civilian Personnel, Appendix A, prescribed by the Department of Defense for travel in Alaska, Hawaii, The Commonwealth of Puerto Rico, and the territories and possessions of the United States;

b. Federal Travel Regulations prescribed by the General Services Administration for travel in the contiguous 48 United States;
c. Standardized Regulations, (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances in Foreign Areas" prescribed by the Department of State, for travel in areas not covered in (a) and (b) above.

Once travel is completed, a travel report confirming costs and travel shall be filed with the monthly status report and referenced when invoiced.

11.0 SECURITY

11.1 The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

11.2 In addition, all contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. In addition, personnel with access to CE production data must have a fully-adjudicated Single Scope Background Investigation (SSBI).

12.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

APPENDICES

Appendix A – Software Development Roadmap
Appendix B – Automation Standard Best Practices
Appendix C – Enterprise QA Roles and Responsibilities
Appendix D – DMDC ARB Charter References (Enclosure 1)
Appendix E – DMDC ARB Charter Required Artifacts (Enclosure 2)
Appendix F – DMDC ARB Charter Process Map and Description (Enclosure 3)
Appendix G – DMDC ARB Charter
Appendix H – CEAS Project Charter
Appendix I – CEAS Reports List
Appendix J – Template Checklist
Appendix O – EHRM Applications

13.0 APPLICABLE DOCUMENTS

Document	Web link
DODI 5000.02 Operation of the Defense Acquisition System	http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002_dodi_2015.pdf
DODI 5200.02 DoD Personnel Security Program	http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520002_2014.pdf
DoDM 5200.02 Procedures for the DoD Personnel Security Program	http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/520002_dodm_2017.pdf
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoDI 8510.01 Risk Management Framework for DoD Information Technology	http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

14.0 CLAUSES

14.1 Data Rights

The Government retains rights to all deliverables/materials (to include editable source files) produced as part of this Task Order, excluding COTS materials. All products developed under this contract shall belong solely to the Government. The government shall have the right to distribute all deliverables under this contract to any person or entity at no cost to the government or the user. There shall be no license or user fees associated with the deliverables under this contract. Products developed under this contract shall not have any commercial license or cost requirements for delivery to other federal, state, and local government customers.
User information supplied to the Contractor for access purposes shall be returned to the Government.
The Contractor shall ensure that all information submitted to the Government is accurate and up-to-date. The Contractor shall support a seamless transition, transparent to the users, with no degradation of services.

14.2 Data Back-ups

The Contractor shall ensure that all data developed for and utilized by contractor staff and Government in the execution of the aforementioned and detailed tasks, is backed-up and protected, so that it can be reconstructed in the event of a catastrophic failure event.

14.3 Section 508 Requirements

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

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of DAU orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http//www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

_x_ § 1194.21 Software applications and operating systems
_x_ § 1194.22 Web-based intranet and internet information and applications
_x_ § 1194.23 Telecommunications products
_x_ § 1194.24 Video and multimedia products
_X_ § 1194.25 Self contained, closed products
_x_ § 1194.26 Desktop and portable computers

The standards do not require the installation of specific accessibility-related software or the Attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services (EITS)
Enterprise Database Administration (ENTDBA)

1.0 INTRODUCTION

The Department of Human Resource Administration (DHRA) and associated field agencies, through the Defense Manpower Data Center (DMDC), require enterprise wide information technology services that can support its full range of IT services in order to develop, sustain and deliver new products, develop and maintain new IT systems, and design, deploy, and maintain the underlying infrastructure. The support will align IT resource expenditures with business goals and objectives and will enable an IT environment with innovative solutions that are responsive to organizational requirements.

2.0 BACKGROUND

2.1 DMDC supports major programs and initiatives within the Department of Defense (DoD) and maintains the largest archive of personnel, manpower, training, security and financial data within the DoD. The personnel data holdings, in particular, are broad in scope and date back to the early 1970's, covering all Uniformed Services, all components of the Total Force (Active, Guard, Reserve, and Civilian), and all phases of the personnel life cycle (accessions through separation/retirement). The categories of data archived at DMDC represent significant data holdings and, in most cases, provide the only single source of commonly coded data on the Uniformed Services. These data support decision-making by the Office of the Secretary of Defense for Personnel and Readiness (OUSD (P&R)), other Office of the Secretary of Defense (OSD) organizations, and a wide variety of customers both within and outside the DoD.

2.2 DMDC operates major programs that include verifying military entitlements and benefits; managing the DoD ID card issuance program; providing identity management for the DoD; helping identify fraud and waste in DoD pay and benefit systems; personnel and property identification, authentication, and access control systems; personnel evacuation support systems; conducting personnel surveys; and assisting military members and their spouses with relocations, quality of life issues and post-service job searches. DMDC is a geographically separated organization with personnel and facilities located in both Virginia (VA) and California (CA) and support offices in Germany, the Republic of Korea, Qatar and Kuwait. The Director of DMDC is located at DMDC's offices in Alexandria, VA.

3.0 SCOPE

The main goal of this Database Administration (DBA) task order is to assure and verify objects deploy correctly to the application-level databases across the DMDC application portfolio.

The contractor shall provide support for the Personnel Data Repository (PDR), Medical Satellite (MEDSAT) and related or dependent databases, systems and capabilities (per Attachment 1), to include:

- Authenticated Data Repository (ADR)
- Authenticated Data Repository Warehouse (ADRW)
- Enterprise Monitoring and Management of Accounts (EMMA)
- Real-time Automated Personnel Identification System (RAPIDS)
- Veteran Affairs (VA)
- Service members Group Life Insurance (SGLI)
- Common Update Framework (CUF)
- Data Governance (DG)
- DMDC Image Management System (DIMS) and DMDC Encounter Tracking System (DETS)
- Database Replication

4.0 REQUIREMENTS: The Contractor shall provide the personnel and management necessary to provide database administration support in accordance with attachment 1, to include:

4.1 Create and maintain Staffing Plan

Provide a Staffing Plan (SP) to the DMDC COR and GSA COR no later than (NLT) 10 business days after award. A copy of the comprehensive written SP shall be submitted to the DMDC COR and GSA COR within 5 business days when changes are made thereafter. The Contractor's SP shall detail the contractor's approach to provide DBA support across DMDC's application portfolio. This approach shall include the contractor's methodology to:

- Continue to provide timely and high quality support when key CTR personnel are out of office or responding to other urgent DBA requirements;
- Provide staffing redundancy to mitigate any deterioration to the timeliness or quality of performance in cases of staff turnover or surge in requirements
- Provide specific details of the required support for application databases on the SIPRNet
- Ensure its staff understands and complies with contractual tasks
- Allocate resources, assign tasks, and plan, direct, control, manage, and monitor tasks across the entire contractual effort

4.2 Provide Project Oversight

4.2.1 Develop project plans and follow industry standard management principles, to include risk management, critical path, resource allocation, stakeholder communication, and milestone reviews.

4.2.2 Escalate priority conflicts to the DBA government leadership for initial review and recommended actions.

4.3 Execute Enterprise DBA Activities.

4.3.1 Collaborate with project teams to provide tablespace sizing estimates for all database objects, and partitioning recommendations. In addition, collaborate across directorates in support of migrations to new technologies and infrastructures e.g. cloud, etc.

4.3.2 Participate in logical database design and modeling. Collaborate with project teams and architects to review proposed application logical data models.

4.3.3 Participate in physical database design requirements. Collaborate with project teams and architects to include these structures for review and inclusion in the physical data model.

4.3.4 Provide database support for all regions (NIPRNet & SIPRNet) through a primary/ secondary on-call personnel hierarchy. Coordinate with the Incident Management group on escalation notification and procedures. Production regions shall be supported 24/7.

4.3.5 Monitor relational database management system (RDBMS) log files proactively for database problems. If problems are found, work with the appropriate application team or the Tech Services Database Team to troubleshoot and remediate the issue.

4.3.6 Collaborate with the Systems team to proactively monitor RDBMS space utilization and request additional space in advance of outages.

4.3.7 Provide a monthly report that indicates the outages due to space incapacity. The report shall include:

- The name of the database requesting additional space
- Databases that were successful in increasing space
- Databases that received outage due to space
- Mitigation for future

4.3.8 Deploy objects into databases on the NIPRNet and SIPRNet through the established DMDC processes and provide verification of deployment. These processes may be found in the Software Delivery Lifecycle (SDLC) Process Handbook outlined in Appendix E.

4.3.9 Provide quality check on updates to databases and assure scripts/ updates to databases have the desired end result. Provide necessary feedback to project teams.

4.3.10 Review database log files for database related problem and provide mitigation.

4.3.11 Design, implement, monitor and tune Structured Query Language (SQL), Data Definition Language (DDL), and Data Manipulation Language (DML) statements stored in the database. Coordinate with Technical Services (TS) System DBAs to obtain Automatic Workload Repository (AWR) reports for databases in order to collect and analyze data to identify problems and determine overall database health. Develop, maintain, and support approved enterprise database objects (including triggers, indexes, data definition language, packages, stored procedures, views, and account profiles).

4.3.12 Ensure that all implemented database objects follow the DMDC development processes, outlined in the SDLC in Appendix E, are stored in the DMDC repository and are under configuration management and version control.

4.3.13 Monitor schema storage consumption and identify storage usage trends.

4.3.14 Provide annual consumption projections of Production application databases by June for the following fiscal year, so that additional storage can be procured, if necessary.

4.3.15 Schedule database object reorganization based on trends.

4.3.16 Assist application teams to identify pending project storage requirements.

4.3.17 Advise Systems team on application container threading as well as database connection pooling information.

4.3.18 Collaborate with Configuration Management (CM) and Enterprise Services and Tech Services teams on deployment policy and process. Once CM provides approved RDBMS objects for deployment, deploy to the respective application/project schema.

4.3.19 Provide Database Restore and Recovery support in collaboration with the Tech Services teams.

4.3.20 Participate in disaster recovery exercises as well as specific 'point in time' recoveries. The DoD Risk Management Framework (RMF) process requires at least one annual disaster recovery exercise. These exercises are performed outside of normal business hours. DMDC anticipates no more than four disaster recovery exercises a year.

4.3.21 Determine the backup start point and the recovery end point in order to restore the database to its proper production state.

4.3.22 Perform database conversions and migrations in support of application changes.

4.3.23 Support, maintain, and keep the test, development, and pre-production databases and database configurations consistent across environments, while providing database refresh of all database instances.

4.3.24 Support data extracts from production databases in response to DMDC Data Requests. Ensure all DMDC privacy policies are enforced when extracting PII.

4.3.25 Assist those in the areas of Data Quality Control and Quality Assurance in verifying the accuracy and completeness of the data in DMDC databases (e.g. Personnel Data Repository (PDR), Joint Verification System (JVS), RAPIDS/CAC). If production data correction is required the correction scripts/programs must be tested in a test or model office prior to being executed in production. All original data should be backed up prior to the production execution and recovery scripts should be coded as well.

4.3.26 Maintain the database maintenance dashboard and reports which monitors task support requests. The contractor shall leverage the existing issue tracking reporting capability, JIRA, for dashboard, trending, and status.

4.3.26.1 Maintain the Standard Operating Procedures (SOP) for the dashboard that outlines the usage of this capability in order to obtain visibility and manage results.

4.3.27 Collaborate with the Tech Services teams to establish/control database security.

4.3.28 Report any unauthorized DDL activities to the appropriate government information assurance officers.

4.3.29 Maintain and operate consistent with all ENTDBA SOP Manuals and checklists, located in Appendix A-D.

4.3.30 Provide feedback to application personnel on how to effectively query database tables. Review and suggest query improvements explaining the rationale behind the changes. Advise them on RDBMS tools which will assist them in constructing efficient database queries. Response time to requests shall be consistent with the SOP outlined in Appendix C: Enterprise DBA Task Request SOP.

4.3.31 Make changes to database replication based on new requirements. Configure, maintain and monitor replication for errors and data consistency.

4.3.32 Verify replicated database synchronization utilizing the appropriate function and resolve any inconsistencies.

4.3.33 Provide ongoing analysis, design, implementation, support, and sustainment of consolidated enterprise database assets that are within scope of this task order.

4.3.34 **OPTIONAL TASK** Support Additional Databases **NTE $250k** (To be definitized at the time of exercising. May exercise more than once based on Attachment 1 OPTIONAL CLIN section).

4.4 Reports and Meetings

4.4.1 Expenditure and Resource Report.

The Contractor shall provide an Expenditure and Resource Report (ERR) to the DMDC COR and GSA COR on a monthly basis. The Contractor shall submit the monthly ERR by the twenty-fifth (25th) calendar day of each quarter. This report shall detail the amount that will be billed to the Government and the resources assigned to each project that is being worked by the contractor in support of this PWS. Each report shall provide details on the previous month, the current month and cumulative task order costs by project.

4.4.2 Ensure all deliverables are submitted to the Government with a completed evaluation checklist. Track returned and completed evaluation checklists from the Government PM to include, accepted checklists, dates, checklists that are not accepted, and the contractor's rewrite submission until the deliverable is accepted.

4.4.3 Maintain the DBA SharePoint site to keep the calendar and point of contacts listed current. All deliverables and artifacts provided shall be maintained on the DBA SharePoint site.

4.4.4 Facilitate and participate in Task Order Kick-Off Meeting within 10 business days of task order award. Distribute Task Order Kick-Off Meeting Minutes notes within 3 business days of Kick-Off Meeting; meeting minutes shall include action item register and shall be executed by the contractor.

4.4.5 In-Progress Review (IPR)

Participate in the weekly IPR conference to discuss on-going project progress, review issues, plan for changes going forward, and address any outstanding action items. These conferences are used to summarize activities that have been performed since the previous call and discuss the status of activities going forward.

4.4.5.1 Maintain the IPR briefings and minutes via the DBA SharePoint site, and/or other communication forums within three business days of the meeting.

4.4.6 Participate in weekly team meetings to discuss technical and operational subjects.

4.4.7 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

5.0 DELIVERABLES

The contractor shall provide the following deliverables and reports, the format of which to be defined or approved by the Government.

Deliverable	PWS Reference	Due Date
Staffing Plan (SP)	4.1	10 business days after task order award, and 5 business days for changes.
Monthly Outage Report	4.3.7	Monthly, NLT 5th working day after the end of the calendar month
Annual Application Schema Usage Estimates	4.3.14	NLT 05/31/20
DBA task request Dashboard Updates	4.3.26	As required
Dashboard Standard Operating Procedures	4.3.26.1	As required
Provide suggested updates to the DBA Standard Operations Procedures	4.3.29	Monthly
Expenditure and Resource Report	4.4.1	Quarterly
Project SharePoint Sites Maintenance	4.4.3	14 business days after task order award and 7 business days after project kick offs. Further changes as needed.
Task Order Kick-Off Meeting Minutes	4.4.4	3 business days from Kick-Off Meeting
Kick-Off Action Item Register	4.4.4	3 business days from Kick-Off Meeting
In-Progress Review Briefing/Minutes	4.4.5.1	Weekly
Senior Management Review (SMR)	4.4.7	15th of each month
Problem Notification Reports (PNR)	6.5	NLT 5 business days after identification of problem

6.0 QUALITY SURVEILLANCE

6.1 The Government reserves the right to perform inspections and surveillance to evaluate the Contractor's compliance to the contract terms and performance of the requirements in the PWS. The Government will make every effort to ensure that the surveillance methods described below are conducted in an objective, fair, and consistent manner.

6.2 Periodic Surveillance. This action occurs when the COR or other Government official observes a deficiency. Examples include evidence from accidents, incidents, or delays. Regardless of where in the line-of-duty the COR observes contractual procedures not being followed, he/she has an obligation to document and report the deficiency to the Contracting Officer.

6.3 Customer Complaint Surveillance. This action is instituted when the COR receives a complaint from a stakeholder (stakeholder organizations include P&R IM, DPRIS User Agencies, Military Service Repository Owners, and the Defense Information Systems Agency) regarding contractor service. The COR will obtain the complaint in writing and then conduct an investigation to determine its validity. If the complaint is deemed valid, the COR will immediately notify the contracting Officer for action. The COR will notify both the Contract Manager and the complainant of the Government's response to their complaint.

6.4 Contract Discrepancy Report (CDR).

The Contractor shall follow the requirements identified in PWS Section 5.8.8 of the EITS II Base IDIQ.

6.5 Problem Notification Reports (PNR)

The Contractor shall follow the requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ

6.6 The table below identifies the Critical Performance Elements and the respective Performance Standards and Acceptable Quality Levels (AQLs) which the Government will use to determine contractor performance. The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation. Failure to meet the performance metrics below will result in negative past performance evaluations.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments.

6.7 Performance Objective and Thresholds:

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection

Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) business days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) business day of initial government notification.	100% inspection
Collaborate with the Systems team to proactively monitor RDBMS space utilization and request additional space in advance of outages.	Requests to increase space shall be made before outage occurs 98% of the time.	100% inspection

6.8 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, will be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

7.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the Contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets, copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

The Government will provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; commercial off-the-shelf software; hosting facilities; and all other relevant materials and equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support.

8.0 PLACE OF PERFORMANCE / HOURS OF OPERATION

The Government requires two full time equivalent (FTE) with Secret security clearances on site at DMDC facilities in Seaside, CA at all times. The remaining percentage of work may be performed in Seaside or by telework. Any work performed at other locations must be identified in the formal submission and approved by the Government. Occasional travel may also be required, as noted in PWS Section 10.0 Contractor Travel.

The contractor is responsible for conducting business between the hours of 8 a.m. ET to 5 p.m. PST, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

9.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order will be 12-months from date of award (with four (4) 12 month option periods).

10.0 CONTRACTOR TRAVEL

The cost reimbursable not-to-exceed travel limit is estimated at **$5,000.00** for each period of performance. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. Before contractor travel is executed, authorization must be given by the DMDC COR and GSA COR.

All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

The contractor shall comply with all security requirements detailed in the base IDIQ contract.

In addition, certain contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances, as directed by the Government. Contractor personnel shall possess these security clearances at Task Order award.

12.0 INSPECTION, ACCEPTANCE AND PAYMENT

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

Delivery Address. All deliverables shall be submitted to the designated DMDC POC's. Additionally, if directed, the Contractor shall upload the deliverables into the GSA ITSS Portal.

Method of Delivery. The Contractor shall provide all deliverables and reports in the format of which to be defined or approved by the Government and subject to change over the course of the task order.

Acceptance Criteria. Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in EITS Contract ID03180056 and all terms and conditions of this Task Order, including all modifications.

Acceptance of Deliverables. The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 calendar days, the Contractor shall not assume

that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 business days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

Invoicing

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Executive Performance Appraisal Tool (EPAT)
Development, Sustainment, and Management

Revision 1

1. INTRODUCTION

The Defense Manpower Data Center (DMDC) requires system development, sustainment, and management support for the Executive Performance Appraisal Tool (EPAT).

2. BACKGROUND

The DMDC Customer Relationship Management (CRM) Directorate has a mission requirement to develop and sustain enterprise tools and applications that comprises the Civilian Personnel IT Portfolio. CRM has an ongoing need for contractor support in the areas of system development, sustainment, management and software implementation.

This support will enable the DMDC CRM to satisfy governance, compliance, development/sustainment, and other mission requirements for the Executive Performance Appraisal Tool (EPAT). Subject Matter Experts (SMEs) are needed to provide program and HR systems support in applying best business practices in enterprise systems lifecycle throughout the Major System Acquisitions and Operation life-cycle.

3. SCOPE

The Contractor shall provide the personnel and management necessary to enable DMDC to successfully develop, sustain, and manage software implementation support for EPAT as identified and detailed in this PWS.

4. REQUIREMENTS

The Contractor shall:

4.1. Provide sustainment and troubleshooting services for the EPAT to include:

4.1.1. Assist in editing content of user guides and training materials related to each system as required with system updates that may affect the accuracy of the artifacts.

4.1.2. Maintain Configuration Management Logs. Configure and setup audit monitoring and logging at the application and database levels for the EPAT servers in accordance to DoD Secure Technical Implementation Guidelines and directives.

4.1.3. Assist in developing and updating specific documentation that supports Cybersecurity Assessment & Authorization.

4.1.4. Assist in updating content of Privacy Impact Assessment (PIA)/System of Records Notice (SORN).

4.1.5. Develop and deploy system improvements, resolve defects, and perform testing in accordance with approved Test Plan.

4.1.6. Conduct security code reviews as part of the software development lifecycle, providing the results to the government Program Managers.

4.1.7. Deploy security and information assurance remediation patches to databases and application software as required and maintain Cybersecurity Plan of Action and Milestones (POA&M).

4.1.8. Ensure EPAT is maintained to operate in compliance with DoD Security Authorization Decision. EPAT is currently hosted at the Denver Data Center (DDC) but is anticipated to be relocated to an Infrastructure as a Service (IAAS) Cloud Environment during the performance of this contract.

4.1.9. **(OPTIONAL)** The Contractor shall be responsible for supporting the application and data move to the IaaS environment. Note: The Contractor will not be responsible for the physical relocation of the EPAT infrastructure.

4.2. (OPTIONAL) Develop and Deploy New Functionality to Transition Senior Level (SL) and Scientific & Technical (ST) Performance Plans by the FY21 Appraisal Cycle:

Development will require the redesign of the plan elements and appraisal forms for, SL, ST, and Defense Intelligence Senior Level (DISL) to a government-wide performance and appraisal system to comply with Government law and regulations.

- U.S. Code Title 5, Part III, Subpart C, Chapter 43, Subchapter II (Performance Appraisal in the Senior Executive Service)
- Code of Federal Regulations (CFR), Title 5, Chapter I, Subchapter B, Part 430, Subpart C (Managing Senior Executive Performance)
- DoD Instruction Volume 1400.25 of the subchapters 920 (SES) and 921 (SP) and 921 (SP) [Executive and Senior Professional Pay and Performance.

The redesign will directly impact the plan elements and appraisal form. The updates include five required elements vice seven optional elements.

These include:

- Three elements which will have numerous possible competencies to choose from a drop down box
- Two elements which are free text.

4.3. Submit Reports

4.3.1. Senior Management Review (SMR)

Provide a monthly Senior Management Review to the Contracting Officer Representative (COR) and designated Government representatives. This review should include data of sufficient detail to monitor the completion of specific work packages against the planned progress as documented in the PWS. The following items shall be included in each review:

- Task Order Summary

- Performance Metrics
- Task Order Schedule
- Hot Items for Government Review
- Accomplishments
- Significant Open Issues, Risk and Mitigation Action
- Summary of Issues Closed
- Meetings Completed
- Projected Meetings
- Subcontractor Performance – discuss 1st Tier subcontractors and Vendor performance
- Projected Activities for Next Reporting Period
- Explanation if the Reporting Period is Over One Month
- Milestone Payment Schedule

The contractor shall deliver the SMR slides by the 15th of each month, reporting on the previous month. The contractor shall schedule the SMR no later than 5 calendar days from delivery of the presentation.

5. DELIVERABLES

Deliverable	PWS Ref.	Delivery Date
User guides and training materials	4.1.1	One week following any significant system enhancement
Configuration management logs	4.1.2	First business day of each month
ATO documentation	4.1.3	Annual basis
PIA/SORN documentation	4.1.4	Annual basis
Test Plan	4.1.5	No later than 30 business days after award
Test report and results	4.1.5	In accordance with approved Test Plan
POA&M documentation	4.1.7	Within 5 business days following each system scan and remediation action
Develop and Deploy New Functionality IAW OPM Policy	4.2	March 2020
Monthly Status Report	4.3	First business day of each month

6. GOVERNMENT FURNISHED PROPERTY/EQUIPMENT

Government will provide office spaces and workstations, computers and telephones when Contractor is required on site. In general, some of the tasks listed above may be accomplished remotely. There are occasional meetings that require on-site presence. In addition, if connectivity or other problems prevent access to the various tools and/or documents listed above, on-site presence may be necessary in order to complete a designated task.

7. PLACE OF PERFORMANCE / HOURS OF OPERATION

DMDC anticipates the majority of work performed will be at the Contractor's facilities. The contractor is responsible for conducting business between the core hours of 8 a.m. to 5 p.m. ET, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The contractor is responsible to hold system releases to complete updates to the system and patches outside of normal business hours monthly or as required.

The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

8. PERIOD OF PERFORMANCE

The Period of Performance for this Task Order is an 8-month base period and two 6-month option periods.

The Government may extend the term of this task order by written notice to the contractor within 30 business days of the expiration of the existing period of performance provided that a preliminary notice of the Government's intent to extend is provided at least 30 business days before the expiration of the task order. The preliminary notice does not commit the Government to an extension.

9. CONTRACTOR TRAVEL

Requirements in this PWS may require travel to the Mark Center in Alexandria, VA for the post award conference. All travel shall be in accordance with FAR 31.205-46 and applicable travel regulations (Joint, Federal or Standardized). Contractor payment claims shall include applicable documentation to support actual costs incurred (e.g. airfare and hotel/lodging receipts) as well as any receipts valued at or above $75.00. Failure to provide appropriate documentation may result in loss of reimbursement of travel expenses.

10. SECURITY

10.1. Perform offsite work with Personally Identifiable Information (PII) only on systems and platform information technology systems (PIT) that meet Risk Management Framework (RMF) (formerly Defense Information Assurance Certification and Accreditation Process (DIACAP)) for DoD Information Technology (IT) requirements.

10.2. Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoDI 8500.01 Cybersecurity. DoD Directive 5400.11 DoD

Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

10.3. Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data.

10.4. Contractor systems and information networks that receive, transmit, store, or process nonpublic Government data must be accredited according to DoDI 8510.01 "Risk Management Framework for DoD IT" (RMF) (formally DIACAP) and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of authorization in the security plan, Security Assessment Report (SAR) Plan of Action and Milestones (POA&M) and authorization decision document or show that the system has successfully went through the Risk Management Framework Process in order to integrate information security and risk management activities into the system's life cycle. The RMF decision must be current and cannot exceed a 3 year timeframe. Evidence FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of RMF processes and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

10.5. Contractor personnel with access to or responsibility for nonpublic Government data under this contract must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must:

10.5.1. Be CAC or PIV ready prior to reporting for work. At minimum all Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check), two forms of identity proofed identification (I-9 document), and submit a National Agency Check and Law Credit (NACLAC) vetting package for processing.

10.5.2. Be citizens of the United States.

10.5.3. Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication of a NACLAC as required for Federal employment.

10.6. If at any time, any Contractor person requiring a CAC is unable to obtain/maintain an adjudicated NACLAC, the Contractor shall immediately notify the DMDC Information Systems Security Group (DISSG) remove such person from work under this contract.

10.7. The Contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach.

10.8. If the position requires elevated administrative privileges or is a Cybersecurity position, the contractor shall possess and maintain certification for all IA/Cybersecurity positions in accordance with DoD Regulation 8570.01-M and all future DoD guidance and directives for Cybersecurity training, certification and education associated with the National Initiative for Cybersecurity Education (NICE) standards.

11. QUALITY SURVEILLANCE

11.1. The Government reserves the right to perform inspections and surveillance to evaluate the Contractor's compliance to the task order terms and performance of the requirements in PWS. The Government will make every effort to ensure that the surveillance methods described below are conducted in an objective, fair, and consistent manner.

11.2. Periodic Surveillance. This action occurs when the COR or other Government official observes a deficiency. Examples include evidence from accidents, incidents, or delays. Regardless of where in the line-of-duty the COR observes contractual procedures not being followed, he/she has an obligation to document and report the deficiency to the Contracting Officer.

11.3. Customer Complaint Surveillance. This action is instituted when the COR receives a complaint from a stakeholder (stakeholder organizations include P&R IM, DPRIS User Agencies, Military Service Repository Owners, and the Defense Information Systems Agency) regarding contractor service. The COR will obtain the complaint in writing and then conduct an investigation to determine its validity. If the complaint is deemed valid, the COR will immediately notify the contracting Officer for action. The COR will notify both the Contract Manager and the complainant of the Government's response to their complaint.

11.4. Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the COR or CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

11.5. Problem Notification Reports (PNR). The contractor shall submit a Problem Notification Report (PNR) to the DMDC PM, GSA COR, and GSA CO within three business days of the contractor encountering a problem or risk event that significantly impacts the cost, schedule, or performance of the Task Order (or any deliverable or project under the Task order). See Attachment 1 for a PNR template. All PNRs must be tracked in the monthly status report (MSR) and through in-progress reviews (IPRs) until the Government agrees they are resolved.

11.6. Critical Performance Elements. The table below identifies the Critical Performance Elements and the respective Performance Standards and Acceptable Quality Levels (AQLs) which the Government will use to determine contractor performance. The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation. Failure to meet the performance metrics below will result in negative past performance evaluations.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments.

Performance Element	Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
Software & Application Sustainment	Ensure a high quality of application and software sustainment	100% compliance, unless forbearance granted by DMDC TPOC	Periodic Surveillance, Customer Complaint Surveillance, Problem Notification Report
Additional	Comply with DMDC's processes	Not less than 95% compliance,	Periodic Surveillance, Customer Complaint

Communications	and procedures	unless forbearance granted by DMDC COR & TPOC	Surveillance, Problem Notification Report
New Software Development	Provide SW Development in design, risk assessment, and systems testing	100% compliance, unless forbearance granted by DMDC TPOC	Periodic Surveillance, Customer Complaint Surveillance, Problem Notification Report
Software Quality Assurance	Comply with contractor's Software QA Plan	100% compliance, unless forbearance granted by DMDC Task Manager or ITM	Periodic Surveillance, Problem Notification Report
Incident Notification and Response	Comply with DMDC notification processes and procedure	100% compliance, unless forbearance granted by DMDC	Periodic Surveillance, Customer Complaint Surveillance

12. QUALITY CONTROL

The contractor shall implement and maintain a Quality Control Plan (QCP) to ensure work performed conforms to the scope of work and meets the requirements under this PWS. The QCP shall, at a minimum provide a method for performing inspections; identifying, correcting and preventing problems/defective service; addressing customer complaints, and improving the quality of services over the life of the contract.

13. APPLICABLE DOCUMENTS

Document - IA	Web link
DoD 5200.01, Vol. 4, February 24, 2012, DoD Information Security Program: Controlled Unclassified Information (CUI)	http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf
DoDI 5200.44, November 5, 2012, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)	http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf
DoDI 8000.01, February 10, 2009, Management of the Department of Defense Information Enterprise	http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf
DoDI 8500.01, March 14, 2014, Cyber Security	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoDI 8510.01, March 12, 2014, Risk Management Framework (RMF) for DoD Information Technology (IT)	http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf
DoDI 8520.02, May 23, 2011, Public Key Infrastructure (PKI) and Public Key (PK) Enabling	http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf
DoDI 8520.03, May 13, 2011, Identify Authentication for Information Systems	http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf

DoD O-8530.01-M, December 17, 2002, Department of Defense Computer Network Defense (CND) Service Provider Certification and Accreditation Program	http://www.dtic.mil/whs/directives/corres/pdf/O853001M_placeholder.pdf
DoDI O-8530.2, March 9, 2001, Support to Computer Network Defense (CND)	http://www.dtic.mil/whs/directives/corres/pdf/O85302p_placeholder.pdf

DoDI 8550.01, September 11, 2012, DoD Internet Services and Internet-Based Capabilities	http://www.dtic.mil/whs/directives/corres/pdf/855001p.pdf
DoDI 8551.01, May 28, 2014, Ports, Protocols and Services (PPSM)	http://www.dtic.mil/whs/directives/corres/pdf/855101p.pdf
DoDD 8570.01, August 15, 2004, Information Assurance (IA) Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf
DoD 8570.01-M, December 19, 2005, Information Assurance Workforce Improvement Program	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
DoDI 8580.1, July 9, 2004, Information Assurance (IA) in the Defense Acquisition System	http://www.dtic.mil/whs/directives/corres/pdf/858001p.pdf
DoDI 8582.01, June 6, 2012, Security of Unclassified DoD Information on Non-DoD Information Systems	http://www.dtic.mil/whs/directives/corres/pdf/858201p.pdf
DoD 5200.2-R, May 6, 1992, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf
DoDD 5400.07, January 2, 2008, DoD Freedom of Information Act	http://www.dtic.mil/whs/directives/corres/pdf/540007p.pdf
DoD 5400.7-R, September 4, 1998, DoD Freedom of Information Act Program	http://www.dtic.mil/whs/directives/corres/pdf/540007r.pdf
DoDD 5400.11, May 14, 2007, DoD Privacy Program	http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf
DoDI 5400.16, February 12, 2009, DoD Privacy Impact Assessment (PIA) Guidance	http://www.dtic.mil/whs/directives/corres/pdf/540016p.pdf
CJCSI 6510.01E, August 15, 2007, Information Assurance (IA) and Computer Network Defense (CND)	http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf
NIST Special Publication (SP) 800-37, February 2012, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems	http://csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication (SP) 800-53, April 30, 2013, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations	http://csrc.nist.gov/publications/PubsSPs.html

DoD 6025.18-R, January 2033, DoD Health Information Privacy Regulation	http://www.dtic.mil/whs/directives/corres/pdf/602518r.pdf

14. INSPECTION, ACCEPTANCE AND PAYMENT

The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this task order. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services.

Delivery Address. All deliverables shall be submitted to the designated DMDC POC's. Additionally, if directed, the Contractor shall upload the deliverables into the GSA ITSS Portal.

Method of Delivery. The Contractor shall provide all deliverables and reports in the format of which to be defined or approved by the Government and subject to change over the course of the task order.

Acceptance Criteria. Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in EITS Contract H98210-13-D-0003 and all terms and conditions of this Task Order, including all modifications.

Acceptance of Deliverables. The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 calendar days, the Contractor shall not assume that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 business days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

Invoicing

The Contractor shall submit Requests for Payments in accordance with requirements below. The Contractor shall provide invoice backup data in accordance with the contract-types established on each Task Order, including detail such as labor categories, rates and quantities of labor hours, and itemized travel, maintenance rates, etc.

The Government reserves the right to audit, thus; the Contractor shall keep on file all backup support documentation for labor, travel, and quarterly maintenance rate adjustments, etc.

The Contractor shall submit a draft or advance copy of an invoice to the DMDC client POC for review prior to submitting such invoice to GSA for payment. The Government reserves the right to require certification by a GSA COR before payment is processed.

Invoice Requirements

The Period of Performance (POP) for each invoice shall be for one calendar month. The Contractor shall submit only one (1) invoice per month. The Contractor shall submit the invoice to the appropriate GSA office by the twenty-fifth (25th) calendar day of the month after the end of the invoiced month for services rendered.

Content of Invoice: The Contractor's invoice shall reflect billings for the services, travel, etc., ordered by GSA and used to support of DMDC. To be considered proper, the invoice shall include the following information at a minimum:

a. GSA Task Order Number (from GSA Form 300, Block 2)
b. Paying Number: (ACT/DAC NO.) (From GSA Form 300, Block 4)
c. ITSS Order ID No.
d. Project Title
e. Remittance Address
f. Period of Performance for Billing Period
g. Point of Contact and Phone Number
h. Itemized invoice data for labor, travel, billed to appropriate CLINs/sub-CLINs/Task Items consistent with the details outlined below with current billed and cumulative billed to date subtotals.
i. Total Invoice Amount, Current Billed, Cumulative Billed to Date

All cost presentations provided by the Contractor shall include general and administrative charges, material handling, fees, and overhead applied consistent with the Contractor's approved price proposal and consistent with DCAA recommendations.

All invoice data shall be reported by CLIN and shall be further subdivided to lower level elements (sub-CLINs and ITSS Task Items) as directed by the Government to permit tracking and reporting of fund expenditures and appropriation data consistent with the requirements of DMDC and DMDC client agencies receiving support under this Task Order. The Contractor shall provide the invoice data in an editable Microsoft Excel spreadsheet using a format reviewed and approved by the Government. The Government reserves the right to modify invoicing requirements at its discretion. The Contractor shall comply with any revised invoicing requirements at no additional cost to the Government.

Final Invoice/Close-out Procedures: Invoices for final payment must be so identified and the Contractor shall submit a final invoice within ninety (90) calendar days after the end of the final Task Order Performance Period. After this submission, no further charges are to be billed. After the final invoice has been paid the Contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

Firm Fixed Price CLINs

On the monthly invoice, Firm Fixed Price (FFP) CLINs shall be billed on the basis of 1/8th of the overall Firm Fixed Price (FFP) established for the CLIN in the Base Period and 1/12th of the overall Firm Fixed Price (FFP) established for the CLIN in the Option Periods. The monthly FFP shall be prorated equitably if a partial month or performance period is encountered.

Travel

The Contractor shall adhere to FAR part 31.205-46 for travel associated with this contract. This shall include all travel requirements associated with temporary duty (TDY) or deployments as required

under this task order, Contractor personnel are authorized to invoice travel related costs at the allowance referenced in FAR part 31.205-46.

Cost incurred for Travel shall be shown on the monthly invoice with travel itemized by individual and trip. The Contractor shall provide travel invoice data on separate worksheets in Microsoft Excel spreadsheet format with the following details. Identify all cumulative travel costs billed by CLIN. The current invoice period's travel detail shall include separate columns and totals and include the following:

a. Travel Authorization Number/Identifier
b. Current invoice period
c. Names of persons traveling
d. Number of travel days
e. Dates of travel
f. Location of travel
g. Number of days per diem charged
h. Per diem rate used
i. Total per diem charged
j. Transportation costs
k. Total charges

ODCs and Incidentals

This Task Order does NOT include any non-travel ODCs.

Credits

If the credit invoice is for the same year of a particular ACT#, the Contractor shall include that credit on a subsequent invoice submission against that same ACT#. If the Contractor is unwilling to offset a subsequent invoice then they must submit a refund check.

When the credit invoice is for a different year, the Contractor shall submit a refund check for that credit invoice.

Invoices that net to a credit balance SHALL NOT be accepted. Instead a refund check must be submitted by the Contractor to GSA accordingly. The refund check shall cite the ACT Number and the period to which the credit pertains. The Contractor shall provide the credit invoice as backup documentation. Do not attach credit invoice in ITSS or on the Finance website. It must be attached to the refund check. The refund check shall be mailed to:

General Services Administration
Finance Division
P.O. Box 70965
Charlotte, NC 28272-0965

Invoice Submission Process

Posting Acceptance Documents: Invoices shall be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COR to electronically accept

and certify services received by the designated DMDC Client Representative (CR). Included with the invoice will be all required backup documentation.

Receiving Agency's Acceptance: The receiving agency has the following options in accepting and certifying services:

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. NOTE: The Government's preference is that receiving agency's acceptance is conducted electronically.

b. On Paper Copy: The client agency may accept and certify services by providing written acceptance with the signature of the authorized client representative and the date of acceptance.

Electronic and/or written acceptance of the invoice by the CR is considered concurrence and acceptance of services

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted. Although this acceptance will occur electronically, acceptance shall be obtained prior to the approval of payment. In order to expedite payment, it is strongly recommended that the contractor continue to include the receiving agency's WRITTEN acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If any invoice is received without the required documentation and, (A) the customer's signed written acceptance OR (B) the customer's electronic acceptance, the invoice shall be rejected in whole or in part as determined by the Government.

To submit an invoice to ITSS for Client Acceptance, follow these steps:

Log onto the Internet URL http://web1.itss.gsa.gov using your assigned username and password once logged in, click on "Create Support Documents".

Once in the Create Support Documents field, you will see a list of awarded task order numbers and a pull down menu that reads <<Select Support Document>>. Select the appropriate task order number by highlighting it, then click on the pull down menu; select "Acceptance Information" and click on the "Create" icon.

You are now on the page where you will enter the delivery date and invoice number—do not use special characters in the invoice number and be sure to use exactly the same invoice number and value for GSA Finance. You have the opportunity to send comments to the client (receiving activity) in the detailed comments block. You must attach an electronic copy of your invoice. Click on the thumbtack "Attach" icon to bring up the attachments page. When you are done attaching the invoice, click on the "Submit" button at the bottom of the page to complete the process.

When the acceptance document is submitted, emails requesting acceptance are automatically sent to both the Client and the GSA Project Manager (PM). They will accept, partially accept, or reject the invoice, normally with explanatory comments. The Client will also indicate the amount approved for payment. The system will automatically notify you, the Contractor, of acceptance or rejection of the invoice.

If you need assistance or have any questions regarding the acceptance and approval process, please contact the ITSS Help Desk at the toll free number 1-877-243-2889. Be sure to have the order number or ACT number available.

Attachment 1

Problem Notification Report (PNR) Template

Problem Notification Report (PNR)

1. Nature and sources of problem:
2. COR was verbally notified on: (date) _____
3. Is action required by the Government? Yes_____ No_____
4. If YES, describe Government action required and date required:
5. Will problem impact delivery schedule? Yes_____ No_____
6. If YES, identify what deliverables will be affected and extent of delay:
7. Can required delivery be brought back on schedule? Yes_____ No_____
8. Describe corrective action needed to resolve problems:
9. When will corrective action be completed?
10. Is increased cost to the Government anticipated? Yes_____ No_____
11. Is increased risk to Government users or customers anticipated? Yes_____ No____
12. Did an information assurance violation or system security breach occur? Yes___ No_____

Performance Work Statement (PWS)
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)

Intelligence and Investigations Support
ORDER ID - ID03180056002

1.0 INTRODUCTION

The Defense Manpower Data Center requires Subject Matter Expertise (SME) and Program Management support for the Intelligence and Investigation (I2).

2.0 BACKGROUND

2.2 The Intelligence and Investigations (I2) Program is responsible for providing liaison and subject matter expertise support to the federal and DoD intelligence and law enforcement community. This support is sensitive for issues of national security and is often conducted in classified settings. The I2 Program provides this support to the I2 community for the entirety of the DMDC portfolio of business lines and Programs and therefore provides a broad service capability ranging from deep technical analysis to high-level functional and operational assessments.

3.0 SCOPE

The Contractor shall provide the personnel and management necessary to support planning, designing, sustaining, developing, and implementing Intelligence and Investigations services for the DMDC portfolio of Business lines and Programs. This also includes providing a breadth of I2 program analysis (to include data and application analysis) support for DMDC programs across the classified DOD and Law Enforcement customer base.

4.0 REQUIREMENTS

The Contractor shall:

4.2 i2 Support

4.2.1 **i2 Baseline Support**

4.2.1.1 Provide subject matter expertise support to DMDC leadership in support of Under Secretary of Defense for Intelligence (USDI) and other federal partners in regards to strategy, business planning and business architecture as it relates and supports the Credentialing and Identity Management Mission. This successful accomplishment of these missions must rely on a strategic liaison with multiple Intelligence and Service organizations that are affected by changes within the DoD identity management and credentialing and access management processes, technologies and methods. Some of the concerns are classified in nature and resident expertise is required to steer or suggest architectural considerations and roadmaps.

4.2.1.2 Provide subject matter expertise and data analysis support to DMDC's identity management, credentialing and access management program. Provide analysis support on a daily and recurring basis for external DoD and Federal law enforcement agencies in support of sensitive investigations. The Government anticipates approximately 20 requests per month during the period of performance. Provide support that enables an overarching awareness of DMDC's identity management, credentialing and access management program achievements.

4.2.1.3 Support specifically the review of data sources ingested into the DMDC identity management architecture as well as other credentialing, and security and reporting systems. Provide analyses as to the operational security of intelligence programs and their impacts on the intelligence community. The government anticipates approximately 50 requests per month for reviews during the period of performance.

4.2.2 Additional i2 Baseline Support – Tier 1 (Optional)

4.2.2.1 Provide subject matter expertise and data analysis support to DMDC's identity management, credentialing and access management program. Provide analysis support on a daily and recurring basis for external DoD and Federal law enforcement agencies in support of sensitive investigations. The Government anticipates approximately 30 requests per month during the period of performance. Provide support that enables an overarching awareness of DMDC's identity management, credentialing and access management program achievements.

4.2.2.2 Support specifically the review data sources ingested into the DMDC identity management architecture as well as other credentialing, security and reporting systems and programs which are, or will be, part of the future roadmap. Provide analyses as to the operational security of intelligence programs and their impacts on the intelligence community. The government anticipates approximately 100 requests per month for reviews during the period of performance.

4.2.3 Additional i2 Baseline Support – Tier 2 (Optional)

4.2.3.1 Provide subject matter expertise and data analysis support to DMDC's identity management, credentialing and access management program. Provide analysis support on a daily and recurring basis for external DoD and Federal law enforcement agencies in support of sensitive investigations. The Government anticipates approximately 40 requests per month during the period of performance. Provide support that enables an overarching awareness of DMDC's identity management, credentialing and access management program achievements.

4.2.3.2 Support specifically the review data sources ingested into the DMDC identity management architecture as well as other credentialing, security and reporting systems and programs which are, or will be, part of the future roadmap. Provide analyses as to the operational security of intelligence programs and their impacts on the intelligence community. The government anticipates approximately 150 requests per month for reviews during the period of performance.

4.2.4 i2 National Customer Support Office - (Optional)

4.2.4.1 Provide Subject Matter Expertise and Program Management support for DMDC’s program office within the Intelligence and Law Enforcements communities for the development of new applications as well as support for existing applications.

4.2.4.2 Provide program management support to include support of an I2 National Customer Support Office. The I2 personnel shall assist the Government in the planning, implementation, and operation of the overall I2 Program. This shall include the coordination, development, and documentation of functional requirements with customers and stakeholders and the creation of a program plan and project plans and schedules.

4.2.4.3 Conduct the system and integration activities such as requirements, design, development and internal development testing for new systems and scope enhancements to existing and evolving systems.

4.2.4.4 Provide expert technical advice, guidance, and recommendations for I2 to DMDC on critical IT issues as it relates to code, implementation, environments, software and hardware.

4.2.4.5 Identify tools and technologies that meet the new software development requirements as well as the DMDC current architectural approach.

4.2.4.6 Ensure changes are recorded in a configuration management database and released software and documentation is archived in a software library.

4.2.4.7 Prepare and execute milestone reviews for requirements, design, development and testing as required by the DMDC division issuing the task order, to ensure the development meets the needs of the Government.

4.2.4.8 Provide Data Analysis support by collaborating with the I2 team and use DMDC data to conduct data management and analyses on behalf of DMDC's customers. Data Analysis support consists of provided quantitative analysis of large databases to:

4.2.4.9 Analyze specifications, formulate programming approaches, and consult with DMDC and its customers to clarify requirements,

4.2.4.10 Analyze incoming data to ensure compliance with the required technical specifications and quality standards for various initiatives,

4.2.4.11 Collaborate with data submitters to manage all data intake. Communicate corrections and recommend any remediation to improve the data analytical value.

4.2.4.12 Provide complete and thorough documentation for functional and technical specifications, data quality reviews, mission security assessments and mission impact assessments; investigate existing databases; research data anomalies, and construct subset data bases and data files.

4.2.5 i2 Program Management Services – Tier 1 (Optional)

4.2.5.1 Provide analytical expertise in identifying, evaluating and documenting business requirements for systems and procedures that meet user requirements.

4.2.5.1.1 Assess and provide recommendations to improve business and IT processes.

4.2.5.1.2 Assess new systems and design methodologies to accurately represent customer requirements and improve software and hardware quality.

4.2.5.1.3 Evaluate and document business processes.

4.2.5.1.4 Enhance and develop existing applications by conducting research related to problem sets, feature sets, and use case limitations for customer project requests.

4.2.5.1.5 Conduct research related to future changes relevant to existing finished and in-process solution products to enable relevance and usability of products over time.

4.2.6 i2 Program Management Services – Tier 2 (Optional)

4.2.6.1 Evaluation of business process, anticipation requirements, uncovering areas for improvement, and developing and implementing solutions.

4.2.6.1.1 Coordinate project(s) to include project definition; requirements negotiation; delivery timelines; priorities; organizational responsibility; software and hardware development; testing and implementation throughout complete product life cycles; and communication with internal/external agencies.

4.2.6.1.2 Monitor project activities, evaluate and report on accomplishments, participate in functional and technical sessions, and provide feedback.

4.2.6.1.3 Manage a portfolio of projects to achieve improved identity management across systems, reducing barriers for adoption by partners, and reducing cost/complexity.

4.2.6.1.4 Create, develop, and maintain required project documents such as file plans, project reports, and continuity binders.

4.2.6.1.5 Create, develop, and maintain necessary solution product documents, including inward-facing documents such as design drafts, production logs and outward-facing technical documentation such as user manuals and customer information pamphlets.

4.2.7 i2 Program Management Services – Tier 3 (Optional)

4.2.7.1 Provide support to the Special Security Office (SSO) for Security Operations.

4.2.7.1.1 Provide security guidance to the SSO by serving as the subject matter expert on sponsors' SCI security requirements as outlined in Intelligence Community Directives and applicable government regulations

4.2.7.1.2 Draft security plans and procedures for submission and approval to the COR.

4.2.7.1.3 Assist with SCI programs, facilities and activities. Administration by serving as the subject matter expert on SCI security requirements.

4.2.7.1.4 Conduct, manage, and coordinate SCI personnel, information, physical and technical security actions and procedures according to applicable security practices and manuals.

4.2.7.1.5 Conduct SCI security briefings, indoctrinations and debriefings; obtain signed non-disclosure agreements and perform related personnel security actions.

4.2.7.1.6 Conduct annual self-inspections. Facilitate prepublication reviews.

4.2.7.1.7 Investigate and resolve SCI security infractions.

4.2.7.1.8 Conduct/perform the following functions:

- Internal audits
- Courier duties.
- Assist with classified meeting preparation
- Support the planning of security education programs
- Assist with interpreting, applying and complying with Security Classification Guides
- Ensure appropriate accreditations are in place for facilities and systems, to include co-use, joint-use agreements and MOUs/MOAs.

4.6 Provide Program Management

4.6.1 Provide business processes that support the integration of activities, maximizing communications among stakeholders while focusing on quality, timeliness, cost efficiency, and accuracy in the delivery of required services.

4.6.2 Business Analysis. Maintain existing government approved business requirements and add additional requirements per the scope of this PWS.

4.6.3 Identify and understand the business problem and the impact of the proposed solution on the organization's operations. Implement training methods and provide training as required.

4.6.4 Document the complex areas of project scope, objectives, and added value or benefit expectations, using an integrated set of analysis and modeling tools.

4.6.5 Evaluate customer business needs, thus contributing to strategic planning of fiscal, information systems and technology directions.
4.6.6 Work with major development and production support teams during preliminary installation and testing of new products and services.

4.6.7 Design and develop high quality business solutions; construct models, process, data, and workflow, develop business architecture: as-is and to-be models and analyze and manage requirement risk.

4.6.8 Structure requirements for traceability, prioritize requirements and draft requirement specifications.

4.7 Project Management

4.7.1 IT project managers support all phases of the software development lifecycle and will follow the DMDC Application Development Process to manage a variety of projects, to include new development, sustainment, infrastructure projects and projects transitioning from and to DMDC infrastructure.

4.7.2 Implement a comprehensive project management approach to include technical management, schedule management, cost management, personnel management, and communication management.

4.7.3 Utilize project management best practices such as those defined in the Project Management Body of Knowledge.

4.7.4 Provide experience in multiple software development project management methodologies, to include waterfall and Scrum/Agile methodologies.

4.7.5 Allocate resource estimates to specific tasks and deliverables or sets of deliverables, including system releases.

4.7.6 Ensure all project management activities are conducted using standardized processes, to include a repeatable SDLC.

4.7.7 Provide project management support to infrastructure projects, to include system maintenance, system upgrades, migrations, and new infrastructure planning and implementation.

4.7.8 Develop project plans and follow industry standard management principles, to include risk management, critical path, resource allocation, stakeholder communication, and milestone reviews.

4.7.9 Assist in evaluating impacts to current schedules and alternative allocations of resources to minimize disruption/impacts introduced by new/changing requirements. Provide updated project schedules within 14 calendar days of changes.

4.8 Provide, Plans, Reports and Documentation

4.8.1 Provide Product Documentation and Reports

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.8.2 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.8.3 Conduct Weekly In-Progress Reviews (IPR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.8.4 Problem Notification Report (PNR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.8.5 Provide a Quality Control Plan (QCP)

- DMDC is committed to a highly interactive relationship between quality control by the Contractor and quality assurance by the government recipient of services. This relationship shall be achieved through a Prevention Based Quality System dedicated to ensuring the best possible products and services. A copy of the comprehensive written QCP shall be submitted to the Contracting Officer (KO) and Contracting Officer's Representative (COR) within 5 business days when changes are made thereafter. The Contractor shall provide their final QCP no later than (NLT) 10 calendar days after contract award.

- The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the contract. The Contractor's QCP shall be incorporated into and become part of this Order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the Order and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the Order.

4.8.6 RISK MANAGEMENT PLAN

The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this contract in a Risk Management Plan. The Risk Management Plan shall be delivered no later than (NLT) 10 calendar days after contract award.

4.8.7 WORK BREAKDOWN STRUCTURE (WBS)

Submit a final detailed Work Breakdown Structure (WBS). The WBS shall detail the decomposition of the work to be executed by the project team to accomplish the project objectives and create the required deliverables in accordance with the statement of work. Define each of the tasks required to complete the work, identify individual responsibilities, and describe output, timelines for completion and performance standards. The Work Breakdown Structure shall identify final completion dates and progress milestones for tasks and provides a basis for monitoring and evaluation contractor work. The WBS shall be delivered no later than (NLT) 10 calendar days after contract award.

4.8.8 Participate in Kick-Off Meeting

This meeting provides an introduction between the Contractor and Government personnel who will be involved with the contract and shall aid both parties in achieving a clear and mutual understanding of all requirements, and identify and resolve any potential issues. This meeting is not a substitute for the contractor to fully understand the work requirements at the time offers were submitted nor is it to be

used to alter the final agreement arrived at in any negotiations leading to contract award. The Contractor shall be prepared to discuss any items requiring clarification and gather information as necessary to support each deliverable and shall submit a written summary of the Kick Off Meeting to the COR. Kick off meeting minutes shall be documented by the contractor and delivered to the Government within 3 business days of the Kick off meeting.

5. DELIVERABLES

The Contractor shall submit a draft version of each deliverable and the Government will provide written acceptance, comments and/or change requests, if any, in accordance with PWS section 5.0. The contractor shall make any corrections and submit the final deliverable, in accordance with the dates listed in the following table and in accordance with PWS section 5.0. The Government will provide written acceptance, comments and/or change requests, if any, within ten (10) business days from Government receipt of the draft deliverable, and sign off on the deliverable check sheet for the final draft of the deliverable within three (3) business days after the due date for submission into GSA ASSIST. After three business days if not approved, the deliverable is deemed acceptable. The work products and reports shall be delivered in accordance with dates listed in the following table:

Deliverables of I2	PWS Ref.	Delivery Date	Date or Recurring
Program Plan	4.2	30 calendar days after award	date
Project Plan	4.2	7 calendar days after project approval	monthly
Requirements Analysis	4.2	as specified in approved project plan	monthly
Functional Specifications	4.2	as specified in approved project plan	monthly
Monthly Status Report	4.8.1	15th of each month	date
QCP	4.8.5	Within 10 calendar days of award	date
Risk Management Plan	4.8.8	Within 10 calendar days of award	date
WBS	4.8.7	Within 10 calendar days of award	date
Kick Off Meeting Minutes	4.8.8	Within 3 business days of meeting	date
Problem Notification Reports	6.0	NLT 5 business days after identification of problem	monthly
Travel Reports	10	Within 5 business days of completed travel	monthly

Weekly IPR	4.8.3	Weekly	monthly

6.0 QUALITY SURVEILLANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

6.7 PERFORAMNCE STANDARDS

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations shall be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations shall contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Quality of Service: deliverables are complete and accurate	No more than one (1) set of corrections required for any product provided for a given deliverable. All corrections submitted within one (1) working day of the negotiated suspense.	100% inspection
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) business days.	100% inspection
Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection

7.0 CONTRACTOR PERSONNEL

The contractor shall provide qualified personnel under this and ensure they possess the skills, knowledge, training required to ensure satisfactory performance of all services required.

8.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

8.1 Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the Contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets, copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

8.2 The Government shall provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; storage media commercial off-the-shelf software; hosting facilities; and all other relevant materials and equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support.

9.0 PLACE/PERIOD OF PERFORMANCE

9.1 Contract Type: This contract shall be Firm Fixed Price.

9.2 Period of Performance: The period of performance (PoP) for this Task Order will be 12 months. Remaining optional Tasks PoP will also be 12 months from the date they are exercised.

9.3 Place of Performance: The work under this task shall be performed on site at DMDC facilities in Seaside, CA. Any work performed at other locations shall be identified in a formal submission and approved by the Physical Security and Law Enforcement (PS&LE) or equivalent DMDC Government division. Occasional to significant travel may also be required, as noted in PWS Section 10.0-Travel.

9.4 Hours of operation: The contractor is responsible for conducting business between the hours of 6 a.m. to 6 p.m.PT, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The Contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task will require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations (if optional CLIN from section 4.2.7 is exercised).

9.5 Post Award Conference: The Contractor shall follow the IPR requirements identified in the PWS Section 10.1 of the EITS II Base IDIQ.

9.6 Telecommuting/Telework: The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The Contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following: Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.

9.7 Points of Contact:

DMDC COR:
Will be assigned Post Award

GSA Contracting Officer (CO)
Mr. Michael Levy
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106

E-mail: Michael.Levy@gsa.gov
Tel: 215-446-5806

GSA Contract Specialist (CS)
Mr. David Long
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: David.Long@gsa.gov
Tel: 215-446-4597

GSA Contracting Officer's Representative (COR)
Mr. Shail Shah
GSA-FAS, Mid-Atlantic Region
The Dow Building - 3rd Floor
100 S. Independence Mall West
Philadelphia, PA 19106
E-mail: Shail.Shah@gsa.gov
Tel: 215-446-5858

10.0 TRAVEL

Travel: The cost reimbursable not-to-exceed travel limit is estimated at $7,500.00 per year. It is noted that the travel costs set forth are estimates and the Government reserves the right to increase or decrease this estimate during performance as necessary to meet requirements. Any travel requirements that arise in excess of the limitations set forth above shall be incorporated through a modification to this task order.

Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs.

Before contractor travel is executed, authorization must be given by the COR.
All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ

In addition, all contractor personnel under this task order shall be fully adjudicated to get a credential and some or all personnel may be required to hold at a minimum a fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. The Government may require some or all personnel under this task to hold a Top Secret with SCI security clearance.

12.0 INVOICING

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf

Task Orders Issued Under

Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II
(EITS II)

Indefinite Delivery Indefinite Quantity (IDIQ) Contract

---

1. Order #: 47QFMA19P0003
2. Order #: 47QFMA19P0005
3. Order #: 47QFMA19P0006
4. Order #: 47QFMA19P0002
5. Order #: 47QFMA19P0001
6. Order #: 47QFMA19P0004
7. Order #: 47QFMA19D0003
8. Order #: 47QFMA19P0007
9. Order #: 47QFMA19F0023
10. Order #: 47QFMA19P0008
11. Order #: 47QFMA19P0009
12. Order #: 47QFMA19F0030
13. Order #: 47QFMA19F0026