Performance Work Statement
Enterprise Program Management Support
Defense Manpower Data Center

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 the full range of information technology-related program management support services.

2.0 BACKGROUND

2.1 DMDC is a component under DHRA, a Department of Defense (DoD) Field Activity. DMDC maintains the central and authoritative store of personnel, manpower, training, and security data for the DoD. DMDC is a geographically separated organization with personnel and facilities located in Alexandria, Virginia; Seaside, California; San Antonio, Texas; Fort Knox, Kentucky; Korea; Southwest Asia; and, Germany. While being geographically dispersed, DMDC takes pride in delivering timely and quality support to the DoD and its members. DMDC supports major programs and initiatives within the DoD and maintains the Defense Enrollment Eligibility Reporting System (DEERS), 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 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's major programs affect individual members of the DoD, as well as, other Federal Departments and Agencies. The programs support Active Duty, Reserve, Guard, and retired military members and their families, as well as, civilian and contractor employees of the DoD. These programs 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 systems; conducting personnel surveys; performing longitudinal and statistical analyses; developing military selection, classification, and language proficiency tests; and assisting military members and their spouses with quality of life issues and transition to civilian life.

2.3 DMDC, based on its expertise and significant data holdings, has been leveraged by the DoD to consolidate like capabilities and deliver enterprise-wide solutions that realize efficiencies for the DoD. DMDC requires an IT environment which provides for operational effectiveness and data-driven decision making while leveraging economies of scale. The future of the DoD's mission superiority relies on solutions which are cloud smart, data centric, and embedded with Zero Trust principles. This model includes a prioritized drive towards greater use of Software as a Service, Platform as a Service, and Infrastructure as a Service, in this priority order of consideration. DMDC is leading the DHRA migration of specific mission capabilities into the desired end state of an integrated "ecosystem" of managed cloud services through a multi-vendor, multi-cloud enterprise environment combining Software as a

Service, General Purpose, and Fit-for-Purpose cloud. This major initiative is being implemented at the same time as additional budget cuts and Defense-wide Reviews are looking for opportunities to streamline and identify efficiencies within the DoD Field Activities. DMDC must reinvent its business process and methods for delivering capabilities to remain relevant and operational in the future.

2.4 DMDC requires ongoing contract support for strategic initiatives and operational programs, including the following:

2.4.1 Joint DoD / Department of Veterans Affairs (VA) Data Strategy and P&R Data Strategy to deliver data dominance meaning strategically ready, globally relevant, and flexibly sustainable P&R enterprise. This requires DMDC excellence as a data-centered organization with a robust IT infrastructure with the ability to rapidly manipulate and exploit voluminous data, to bring insight to senior leaders in real-time at the speed of relevance. The Joint Data & Analytics Strategy and Implementation Plan has been established to strengthen VA/DoD collaboration, capitalize on best practices and existing investments, and pursue a federated data approach. DoD and VA are partnering to implement a federated mesh of well-governed, decentralized data products made securely available across the DoD-VA ecosystem to reduce data movement and deliver the right data at the right time and establish a federated catalog of data assets in the joint space to ease the burden of discovery, understanding, and exchanging data across all domains

2.4.2 Joint DoD-VA next-generation Electronic Health Record (EHR) system to enable in all patient data to reside in one common system. DMDC provides a set of services to provide identity, demographics, eligibility, and Other Health Insurance, immunization data, and self-service login (DSLOGON) to the DoD EHR implantation today. In support of a joint implementation of a single EHR system by the DoD and the VA, DMDC requires expertise in patient identity and Cerner Electronic Health Record Products to support integration of identity and potential other services with the Defense Health Agency (DHA) and the VA.

2.4.3 Human Resource Management (HRM) Functional Strategy and Portfolio Rationalization to oversee and enable strategic investment decision-making. An HRM portfolio analysis has been completed to document all HRM Business Mission Area (BMA) systems and interfaces in order to visualize the current HRM IT Portfolio. This analysis has been incorporated into the HRM Functional Strategy to help the DoD realize its strategic goals, objectives and priorities to deliver HRM capabilities to the DoD. DMDC, as the key strategic lead for the HRM Functional Strategy across the Fourth Estate and Military Services, must engage stakeholders to execute HRM initiatives to help the Department realize it desired future state.

2.4.4 In August 2020, DoD CIO published the DoD Identity, Credential, and Access Management (ICAM) Reference Design. This document includes specific development activities for DMDC to transform legacy DoD identity capabilities into a modern data-centric identity-based access management architecture, required to support a future-state Zero Trust (ZT) Architecture. DMDC has been tasked to re-engineer existing enterprise capabilities and initiate new DoD enterprise capabilities to facilitate cloud-native ICAM capabilities, auditability, the right access decisions, and the use of artificial intelligence and machine learning to reduce and better prevent fraud and insider threat. To deliver these artifacts in support of the establishment of new identity programs, architectures, and capabilities within the DoD enterprise ICAM-space, DMDC requires expertise of public key infrastructure, identity attributes, identity programs, credentialing programs, and identity and access management (IDAM) principles,

policies and practices to develop the program documentation to support the functionality and capabilities required by DoD and its mission partners (See Appendix L).

2.4.5 The Real-time Automated Personnel Identification System (RAPIDS) issues DoD and Federally mandated identification (ID) card issuance for all DoD active duty, guard/reserve, DoD civilians and contractors enabling logical and physical access to DoD assets, and ID cards for eligible family member enrollment for benefits and entitlements. The RAPIDS program requires engineering expertise to support the current capability with workstations deployed globally and credentialing expertise of industry best practices to analyze alternatives for transforming the legacy solution into a web-enabled architecture that can meet DoD unique mission requirements.

2.4.6 Physical Access Control capabilities working in close partnership with the Physical Security Enterprise & Analysis Group (PSEAG). The Defense Biometric Identification System (DBIDS) is an identity management and force protection system designed to manage personnel, property and installation access for the Department. DBIDS uses a combination of biometric information and personnel Identity credentials (including Common Access Cards (CAC), Uniformed Services Identification (USID) cards, and other Federal Agency Personal Identity Verification (PIV) cards) to verify identity and access rights. Identity Matching Engine for Security and Analysis (IMESA) currently delivers law enforcement and other pertinent security data to DoD physical access control systems for real-time fitness vetting of more than 10 million DoD and non-DoD credential holders when attempting to gain installation access.

2.4.7 Personnel Accountability applications and services to include Synchronized Pre-deployment and Operational Tracker (SPOT), Noncombatant Evacuation Operations (NEO) Tracking System (NTS) (OCONUS) and Emergency Tracking Accountability System (ETAS) (CONUS), the Joint Asset Movement Management System (JAMMS), the Joint Personnel Accountability Reconciliation and Reporting System (JPARR), Personnel Accountability Reporting System (PARS).

3.0 OBJECTIVE

The objective is to acquire the full range of information technology-related program management support services, to assist in establishing and maturing the DMDC service delivery model by implementing program management best practices that reduce cost and complexity of IT systems and applications, to increase the resiliency, adaptability and agility of DMDC's systems and to improve collaboration and cooperation with the Lines of Business, while achieving DMDC's strategic mission objectives (see Appendix A). The nature of this work shall require the Contractor to be capable of quickly responding to stringent deadlines. All work shall fall under the below Task Areas:

- IT Capital and Strategic Planning (4.1)
- Portfolio and Investment Management (4.2)
- Business and System Requirements Management (4.3)
- Policy and Program Management (4.4)
- Program Advisory and Assistance for Research and Development Initiatives (4.5)
- Communication, Knowledge Management and Process Improvement (4.6)
- Customer Service and Relationship Management (4.7)
- Data Governance (4.8)
- Systems Engineering (4.9)
- Contract Management (4.10)

- Surge Support (4.11)

4.0 REQUIREMENTS / TASKS

The Contractor shall provide support of the following tasks:

4.1 IT Capital and Strategic Planning (T&M)

4.1.1 The Contractor shall support strategic planning efforts across designated DMDC program areas, to include planning analysis, documentation, communication and recommendations in support of the DHRA portfolio. Provide expertise in DoD policy, public key infrastructure, identity attributes, identity programs, patient identity, Cerner Electronic Health Record Products, credentialing programs, identity and access management (IDAM), Active and Reserve Component regulatory and statutory personnel and pay requirements impacting DMDC programs development and implementation and human capital planning. Strategic Planning Support shall include the following:

4.1.1.1 Analyze requirements and internal systems for strategic value and performance.

4.1.1.2 Develop technical mapping of systems and applications.

4.1.1.3 Analyze the portfolio to identify similar values and interest areas across systems to enable the management of stakeholder groups in Performance Reviews.

4.1.1.4 Update and coordinate strategic planning documentation and presentations.

4.1.1.5 Facilitate senior executive governance forums (i.e., Quarterly Strategic Planning and Executive Governance Committee) including capturing minutes and tracking action items.

4.1.1.6 Outline, track and report on existing DHRA capabilities and requirements.

4.1.1.7 Develop governance artifacts and processes to ensure input across Components and promote investment transparency.

4.1.1.8 Analyze portfolio human capital resourcing to develop a comprehensive plan to guide mapping and developmental progression to ensure strategic optimization of programmatic effectiveness and asset retention.

4.2 Portfolio and Investment Management (FFP)

4.2.1 Facilitate portfolio management governance forums (i.e., In-Progress Reviews (IPR), HRM Business Council) as required for performance reviews and BCAC milestones to enable portfolio IT investment planning, management, and optimization. Record and track action items identified in governance meetings.

4.2.1.1 Plan, schedule, and develop presentations required to support IPR meetings to conduct milestone/acquisition decision reviews or other investment related reviews. Maintain Portfolio and Investment Strategic Calendar on SharePoint.

4.2.1.2 Track and report on new capability requirements development and existing capabilities / requirements.

4.2.1.3 Incorporate changes from broader DoD business process reengineering into DHRA processes.

4.2.1.4 Develop governance artifacts and processes to ensure input across USD P&R and promote investment transparency.

4.2.1.5 Perform enterprise level program planning and metrics analysis to facilitate better investment decision-making by the HRM Business Council.

4.2.2 Support the evaluation of the DHRA IT system portfolio to identify functionality and technology rationalization opportunities; support system-level business case analysis and recommend investment opportunities that would make the systems in the portfolio more efficient and effective in supporting the HRM Strategies and business mission needs.

4.2.2.1 Provide technical and costs analysis input to the Government on the portfolio of Defense Business Systems (DBS) for compliance with laws, regulations, directives, and policies to ensure alignment of the portfolio of systems to the business capabilities defined in the business enterprise architecture, and to manage current and future IT investments.

4.2.2.2 Perform cost/benefit analyses, affordability analyses, cost estimating drills, economic analyses, and other cost assessments (which could include either return on investment (ROI) or statistical analysis dependent on the item under review) to support the recommendations.

4.2.3 Prepare, document, and coordinate with internal and external organizations to support the processes in business capability acquisition cycle (BCAC) IAW DoDI 5000.75.

4.2.3.1 Assist with the development of the evaluation phase criteria for CIO, DHRA approval and execute the phase to determine if the DBS delivered the intended outcomes and benefits. During the evaluation phase, fundamental questions must be answered, corrective actions taken, and schedules identified.

4.2.4 Support the staffing and submission of PfM documentation (see Appendix J document titled *"Interim ITSM Handbook – PfM.V8-01.01.18")* for review and approval, to include reviewing, staffing, and publishing all acquisition and milestone documents.

4.2.5 Assist in the preparation of annual Program Objective Memorandum (POM) and Planning, Programming, Budgeting and Execution (PPBE) documentation.

4.2.5.1 Build out Technology Business Management (TBM) Taxonomy to support modeling of costs and other key metrics

4.2.5.2 Track investments and cost savings to demonstrate return on investment for the portfolio management processes

4.2.5.3 Develop cost estimating models and life cycle cost estimates and provide to the Government Program Managers for inclusion into POM IT worksheets and to facilitate the requirements management process.

4.2.5.4 Analyze POM submissions across the DHRA Portfolio with IT equities to evaluate alignment with DHRA strategic goals and compliance with DoD and DHRA Policies.

4.2.5.6 Implement procedures to monitor technical, cost, and schedule performance; establish metrics to assess and report project status in order to and predict deviations from the planned or required performance (cost, technical, or schedule) in sufficient time to take corrective action.

4.2.5.7 Assist in budget formulation, submission, and reporting of designated DHRA programs and IT investments.

4.2.5.8 Coordinate the development of viable financial spend plans and monitor the execution of financial spend plans, including reimbursable funds and their impact against resources.

4.2.5.9 Develop standard procedures for documenting and reporting the IT portfolio costs.

4.2.6 Support DHRA IT Investment oversight, reporting and compliance with DoD policies

4.2.6.1 Facilitate the creation of new IT investments in DITIP, DITPR, and SNAP-IT.

4.2.6.2 Coordinate with DoD CIO on to understand annual IT Budget Guidance and assist DHRA staff in understanding and review DHRA investments to evaluate compliance with DoD policies and guidance.

4.2.6.3 Support the review of IT Investment certification and annual review packages from program managers to ensure submissions are complete and all requirements have been met.

4.2.6.4 Develop draft IT Investment Certification Package, coordination memoranda and supporting documentation for endorsement by the CIO, Comptroller, and the USD P&R Principal Staff Assistant (PSA), as required.

4.2.6.5 Coordinate and review the annual submission of the IT Budget in SNAP-IT, including ensuring correct alignment to TBM taxonomy and identifying data inconsistencies. Coordinate issue resolution with program managers.

4.2.6.6 Identify resolution for system audit errors in SNAP-IT data loads and update submissions.

4.2.6.7 Assist in the preparation of Out of Cycle Certification (OOC) request packages for Pre-Certification Authority (PCA) approval and submission to the Defense Business Council (DBC) if required.

4.2.6.8 Review and identify HRM portfolio equities for all non-USD P&R OOC requests.

4.2.7 Support the maintenance, configuration, and management of portfolio processes and data in the DHRA enterprise business tool. Support training and account management of the Portfolio Module.

4.2.8 Support the Annual Update to the HRM Functional Strategy

4.2.8.1 Assist with the Functional Strategy timelines and schedules, development instructions, coordination of workgroup meetings, and associated correspondence management.

4.2.8.2 Assist with compiling, analyzing, coordinating, and refining Functional Strategy inputs for goals, priorities, initiatives, milestones, and measures.

4.2.8.3 Assist in developing, structuring, coordinating, staffing, and adjudicating the final FS updates.

4.3 Business and System Requirements Management (T&M)

4.3.1 Evaluate trends and forecast projections, for schedule efficiency, and notify the DMDC program manager well in advance of potential negative project impacts.

4.3.2 Develops and maintains standard operating procedures and templates for artifacts referenced in task 4.4.

4.3.3 Prepare and Maintain an Integrated Master Schedule (IMS) using DMDC approved tools and business processes. As directed by the DMDC project lead based on mission priorities, the contractor shall –

4.3.3.1 Prepare and manage a Work Breakdown Structure (WBS)-based IMS for programs/projects through the utilization of any Government Furnished scheduling software used.

4.3.3.2 Participate in IMS reviews of risks and issues in coordination with the Independent Validation and Verification (IV&V) contractor, System Integrator (SI), and Functional and PM Government teams.

4.3.3.3 Coordinate with the System Integrator to maintain the IMS by providing input.

4.3.3.4 Assist in determining the impact of proposed changes to project schedules, project operations, resources, software configurations, and modifications.

4.3.3.5 Review all outputs of draft/final system integrators schedules for completeness and technical accuracy

4.3.3.6 Schedule and coordinate tasks amongst Integrated Product Teams (IPTs) / Working IPTs (WIPTs).

4.3.3.7 Ensure each program/project IMS encompasses all deliverables and resources required within the scope of the project.

4.3.3.8 Ensure dependencies are properly integrated into the IMS and that a critical path can be identified.

4.3.3.9 Ensure activities are included for all disciplines and support functions.

4.3.3.10 Ensure inclusion of all program documentation requirements.

4.3.3.11 Relate schedules to the Work Breakdown Structure (WBS) clearly defining when all tasks start and finish.

4.3.3.12 Maintain the portfolio of DMDC programs/projects in the IMS as the day-to-day tool for planning, executing, and tracking program technical, schedule, and cost status, including risk mitigation efforts.

4.3.3.13 Produce weekly IMS status reports.

4.3.3.14 Coordinate scheduled activities to complete program or project objectives

4.3.3.15 Develop and manage a comprehensive schedule of contractual, modernization activities and infrastructure upgrades.

4.3.4 The Contractor shall provide the following requirements support:

4.3.4.1 Develop high level requirements and decompose functional requirements into technical requirements.

4.3.4.1.1 Support the program office in gathering customer requirements and develop written technical requirements for web services and mobile applications.

4.3.4.2 Design, implement, and manage a process to track and trace requirements, ensuring traceability matrices of requirements from high level requirements to Test cases to Application component.

4.3.4.3 Develop Use Cases

4.3.4.4 Interact with other stakeholders in the requirements process.

4.3.4.5 Perform business process modeling (BPMN) for designated business areas (e.g. patient identity).

4.3.4.6 Assess requirements for testability.

4.3.4.7 Prepare appropriate supporting documents, reports, and presentations in support of the requirements process.

4.3.4.7.1 Develop documentation required for governance processes.

4.3.4.8 Perform technical reviews of requirements products.

4.3.4.9 Assist in the planning, preparation, and conduct of requirements reviews (i.e., SFR, SRR), to include defining entrance and exit criteria.

4.3.4.10 Assist in the preparation of contract documentation to include Request for Proposal (RFP), Statement of Objectives (SOO), and Statement of Work (SOW).

4.3.4.11 Review various technical proposals, analyses and/or solutions to determine if they satisfy DMDC technical requirements and provide recommendations. Anticipate changes in system requirements and bring forth solutions or recommendations for improvements.

4.3.4.12 Validate completeness of engineering change proposals (ECPs) according to the Government Services Agency (GSA) pricing standards and product test reports. Track ECPs throughout the process, ensuring they are incorporated into the Consolidated Equipment Schedule (CES).

4.3.4.13 Assist in developing COTS acceptance packages for government approval. Acceptance packages include an ECP, all applicable test reports, an analysis of the cost benefit, and price verifications. See Appendix H.

4.3.4.14 Monitor state-of-the-art computer, security, telecommunications, biometrics, PKI implementation technologies, and business process improvement techniques for designated programs. Deliver annual report of trends and impacts as it relates to DMDC's strengths, weaknesses, opportunities, and threats.

4.3.4.15 Provide support for configuration control boards, facilitate preliminary design reviews, critical design reviews and other program level governance processes.

4.4 Policy and Program Management (T&M)

As directed by the project lead based on mission priorities, the contractor shall –

4.4.1 Prepare and assist in the development of policy and procedures for program-level management and promote consistency in program management best practices across DMDC programs (the Government is responsible for approving all policies). Provide expertise on DoD policy, public key infrastructure, identity attributes, identity programs, patient identity, Cerner Electronic Health Record Products, credentialing programs, physical security programs, identity and access management (IDAM), Active and Reserve Component regulatory and statutory personnel and pay requirements impacting DMDC programs development and implementation.

4.4.2 Assist in the development of proposed draft policy changes required to meet DoD and VA requirements ensuring it is consistent with the DoD, DHRA and DMDC vision, strategy, and direction/mandates.

4.4.3 Update policies, document technical research, evaluate studies, create staffing packages and manage coordination of policies in accordance with the Department of Defense Manual 5110.04-M-V1 (DoD Manual for Written Material: Correspondence Management), the DoD organizational structure; and knowledge of DMDC information technology solutions.

4.4.4 Prepare and assist in the development of business justifications, program of record and program management artifacts, comprehensive plans, programs, and special reports.

4.4.4.1 Assist in the development and implementation of program governance processes.

4.4.4.2 Facilitate business process re-engineering activities for customer requirements to include DoD/VA interoperability and standardize delivery of DMDC products and services. Document Standard Operating Procedures (SOPs) for applications and processes.

4.4.5 Prepare for and conduct monthly communications reviews covering planning, objectives, risks, and accomplishments. Assist the DMDC leadership in reviewing project progress monthly, documenting issues, and monitoring their resolution.

4.4.5.1 Assist with preparing the documentation required for In Progress Reviews (IPR) or other senior level presentations regarding program cost, schedule, and performance.

4.4.5.2 Provide program management support in compliance with DHRA/DMDC portfolio management processes and tools.

4.4.5.3 Provide programmatic metrics for making decision on effectiveness and efficiency of programs/projects.

4.4.6 Develop processes and procedures to monitor risk, maintain a Risk Management Plan (RMP) template and Risk Register to be implemented by program managers across designated DMDC programs/projects.

4.4.7 Perform risk, threat and vulnerability assessments to identify, define, analyze and respond to program or project issues in terms of cost, schedule, and performance impacts.

4.4.8 Correlate identified risks to data sources, including systems engineering documentation, life-cycle cost analysis, project plan/Work Breakdown Structures (WBS) decomposition, schedule analysis, baseline cost estimates, requirements documents, trade studies/analyses, technical performance measures, and decision drivers.

4.4.9 Conduct and document external and internal stakeholder analysis.

4.4.10 Develop white papers, decision papers, feasibility studies, assessments, briefings, and other documentation as needed on programs, projects or products.

4.4.11 Research, collect, analyze, and validate data to develop briefings, presentations and formal responses to requests for information from Congress, the Office of Management and Budget (OMB), the Secretary of Defense (OSD), other Principle Staff Agencies (PSA), Inspector General (IG), General Accounting Office (GAO), Office of General Counsel (OGC), General Services Administration (GSA), the DoD Military Departments and other agencies.

4.4.12 Analyze data assets and document authoritative sources.

4.4.13 Support Data Governance forums, maintain data activities roadmap, and track / report on the status of the Joint DoD VA Data strategy and implementation plan.

4.4.14 Provide expert advisory support to support DMDC's participation at Federal, DoD, VA and industry forums, including DoD PKI Program Management Office (PMO) initiatives, Federal CIO Council, and National Institutes of Standards and Technology (NIST). Inform DMDC of emerging standards, regulations, and policies that may affect DMDC programs.

4.4.15 Facilitate, participate and provide logistics support to ICAM working groups for: PKI/Public Key Enabled (PKE), logical and physical access, credential management, biometrics, Identity and Access Management (IdM) services to include authentication, authorization, federation, and role/attribute-based access control, ICAM Roadmap and Implementation Guidance, to include the Segment Architecture, Homeland Security Presidential Directive's (HSPD), Wireless Policy, Certificate Management, SIPRNET PKI polices, PKI certificate reduction, Federal Information Policy Standards (FIPS) and associated Special Publications for identity, identity attributes and access management as deemed pertinent by DMDC.

4.4.16 Provide support for various external, intra- and inter Departmental working and decision-making groups and committees such as: the Identity Protection and Management Senior Coordinating Group (IPMSCG), Configuration Management Working Group (CMWG), Defense Security Enterprise Advisory Group (DSEAG),the Test and Evaluation Working Group (TEWG), the Joint Uniformed Services Personnel and Medical Advisory Committee (JUSPAC/MAC), Non-Combatant Tracking System (NTS), Federation Interoperability Working Group (FIWG), Interagency Advisory Board (IAB), Identity, Credential, and Access Management Sub-Committee (ICAMSC), Synchronized Pre-deployment and Operational Tracker (SPOT), CHRM IT Executive Steering Committee, DoD PKI PMO and National Security Agency NSA One Token One Infrastructure (IT/OI), VA/DOD Joint Executive Committee, VA/DOD Benefits Executive Committee, DoD/VA Interagency IT Steering Committee, and Joint Information Environment (JIE), DoD/VA Architecture Working Group, Federal Identity Working Group, DoD/VA JEHR working groups for Patient Identity, Patient Credentials and Access Management, Provider Credentials and Access Management.

4.4.17 The Contractor shall perform and manage Strategic Communications for designated programs, to include coordination with USD P&R, DHRA the financial communities of interest, other stakeholders, and industry partners.

4.4.17.1 Prepare and maintain a programmatic strategic communications plan.

4.4.17.2 Develop PM strategic messages, both internally and externally.

4.4.18 Prepare materials for Congressional responses/testimony/reports, town halls, conferences, demonstrations, literature research, public affairs reports, and liaison with the press.

4.4.19 Coordinate program status review meetings with stakeholders. Coordinate the agendas, assist with the development of the associated presentations, prepare minutes and track/close out action items, and identify overarching program issues.

4.4.20 Design and implement corrective action procedures to prevent, circumvent, or mitigate the impact of deviations from planned or required performance.

4.4.21 Assist in the development of responses to DoD Inspector General, GAO, and various external audit agencies.

4.5 Program Advisory and Assistance for Research and Development Initiatives (T&M RDTE)

4.5.1 Support for RDT&E funded initiatives for tasks described under paragraph 4.4.

4.5.2 Develop outyear project milestone and execution plans for portfolio or program modernization. Plans and project schedules should be captured in the DMDC enterprise tool (i.e., project center).

4.5.3 Develop a resource plan which details projects costs, funding method, and personnel requirements. The resource plan should account for the fully burdened project costs by phase or major deliverable.

4.5.4 Align target state capabilities and processes to DMDC and DoD Business Enterprise Architecture (BEA).

4.5.5 Prepare, document, and coordinate with internal and external organizations to support the processes in business capability acquisition cycle (BCAC) IAW DoDI 5000.75.

4.5.6 Support the staffing and submission of BCAC documentation and milestone decisions for review and approval, to include reviewing, finalizing, presenting to governance forums, obtaining signatures, and publishing all acquisition and milestone documents

4.5.7 Provide detailed steps, by decomposing target state features and objectives, to enable DMDC to transition to future-state architecture and to-be models.

4.5.8 Identify dependencies, decision points, pilot requirements, and risks across objectives detailed in the execution plan.

4.5.9 Prioritize and sequentially place target state features and objectives across the FYDP and identify opportunities for quick wins.

4.5.10 Use a standard approach to implement new services and modernize existing services.

4.5.11 Follow DMDC change control and governance process for the transformation of DMDC's current state to target state

4.5.12 Coordinate efforts of the project teams for planning, organizing, and controlling the development of project deliverables.

4.5.13 Develop, test, receive governance approval and implement Master Data Management standards.

4.5.13.1 Develop data management disciplines in alignment with DMBOK to institutionalize, modernize and automate data management practices.

4.5.13.2 Develop and pilot National Information Exchange Model (NIEM) implementation within the HRM IT Portfolio, upon successful pilot completion follow governance approval process for new standard implementation.

4.5.13.3 Institute new processes and capabilities to perform metadata tagging.

4.5.13.4 Architect and establish a methodology to implement metadata tagging into data transport.

4.6 Communication, Knowledge Management and Process Improvement (FFP – Optional)

4.6.1 Coordinate and assist in the development/revision of Standard Operating Procedures (SOP), policies, and memorandums as necessary and appropriate for smooth operation of the programs.

4.6.1.1 Assist in developing and implementing new business processes, methods, and standards or improve existing IT service management capabilities to mature the service delivery model, including existing best practices, templates and automation. The Contractor shall 1) document processes; 2) conduct customized training sessions on processes; and 3) coach process managers on implementation and sustainment of business processes.

4.6.1.2 Facilitate process and project reviews to kick-off new CPI initiatives or review initiative status The Contractor shall assist with reviewing project documentation, developing project performance measures and reports, facilitating meetings, and tracking and reporting post-meeting actions.

4.6.2 Leverage SharePoint to manage all documentation across all project areas to include ensuring compliance with templates, required content, and staffing procedures.

4.6.2.1 Maintain version control and updates of all documentation delivered to the Government.

4.6.3 Maintain SharePoint sites and electronic libraries where authorized internal and external users may access materials.

4.6.4 Perform business process modeling (BPMN) and integration across DMDC enterprise using the DMDC enterprise architecture tool.

4.6.5 Provide planning and communications support, to include developing the necessary materials and conducting the necessary forums (e.g., briefings, software demonstrations, user workshops, and

marketing materials) to increase the awareness and understanding of external users regarding program objectives and strategies.

4.6.6 Develop and maintain internal and external distribution lists for topics, programs, and projects.

4.6.7 Develop solutions and processes to ensure timely, accurate and effective collection, formatting, dissemination, storage, and disposition of program/project/product information.

4.6.8.1. Assist in the development of strategic management dashboards for designated programs, produce monthly reports, brief strategic goals monthly and track progress.

4.6.8.2 Develop and maintain user stories for strategic dashboards and process integration.

4.6.9 Support DHRA governance processes by integrating and tracking requirements and projects throughout the process. Identify process gaps and escalate requirements that are meeting KPI standards for governance reviews in accordance with the DHRA Governance User Guide.

4.7 Customer Service and Relationship Management (FFP – Optional)

4.7.1 Prepare and assist in the development, staffing, implementation, and maintenance of agreements with external organizations and system owners (e.g., external interfaces).

4.7.2 Conduct outreach sessions with DMDC stakeholders to establish and cultivate relationships with Government and industry to enable mission success for project-wide efficiencies.

4.7.3 Assist Program/Project/Product Managers in preparation for external engagements with stakeholders (e.g. DoD forums, Acquisition/Program Reviews).

4.7.4 Manage day-to-day operations for staffing and maintenance of customer agreements, including tracking the status and prioritizing agreements for review.

4.7.4.1 Maintain agreements dashboard in designated tool.

4.7.4.2 Create status reports and coordinate with Program Managers to ensure that agreements are staffed in accordance with DHRA Operating Instructions.

4.7.5 Assist in drafting and editing of customer agreements. Facilitate training and user guides on agreement policies and process requirements.

4.7.6 Maintain process SOPs and workflows and identify opportunities to streamline or enhance processes for into designated tools to support process automation activities.

4.8 Data Governance (T&M – Optional)

4.8.1 Provide support for the Data Governance Boards and processes, including planning, scheduling, and developing presentations, recording and tracking action items identified in governance meetings.

4.8.2 Maintain queries, analyze, and report on metadata to include data quality metadata, data lineage, and change impacts. (Begins upon delivery of the MDM solutions)

4.8.3 Perform Master Data Management, by maintaining and populating a business glossary and data lineage repository to include the documentation of the standards for validating attribute data when collected, transformed or shared. (Begins upon delivery of the MDM solutions)

4.8.4 Perform Metadata tagging for descriptive, structural and administrative metadata on DMDC's personnel data. This must conform to relevant standards (i.e., NIEM, X12, HL7). (Begins upon delivery of the MDM solutions)

4.8.5 Identify and assess reference data sources and contributors to include required frequency of updates to business glossary.

4.8.6 Establish standards for access to and data exchange for the master data management and metadata repositories.

4.8.7 Provide data governance and master data management (MDM) expertise for activities related to migrating from on-premises applications to cloud services.

4.8.8 Consolidate all Master Data Management information to new tool once selected, including metadata, business glossary, data lineage, data governance workflows, diagrams, policies and others. (Begins upon delivery of the MDM solutions)

4.9 Systems Engineering (FFP)

4.9.1 The Contractor shall provide systems engineering (SE) support to assess and oversee the high level technical requirements, advisory support on preliminary architecture, design and advisory assessment of risk associated with proposed technical approaches of system integrators.

4.9.2 Support applications and hardware test process for operationally fielded systems such as RAPIDS, DBIDS, JAMMS and NTS in production environments. DMDC identifies system application and hardware integration changes that require testing beyond internal quality assurance testing. Provide system and application test support to end-user beta testing and/or user acceptance testing of specified systems. Examples of a major RAPIDS Release Test Report, Test Matrix, and Issue Log are available in Appendix C, Appendix D and Appendix E respectively.

4.9.3 Develop and execute all test activities needed to effectively evaluate the system's performance in a field environment to determine the successful integration of hardware and application changes.

4.9.4 Maintain a functioning production RAPIDS site with fielded and test equipment and software at DMDC. Operate the RAPIDS site in a production environment, following all security, policy, and business process requirements. The contractor supports beta testing activities including user acceptance testing.

4.9.5 Maintain valid user certification on supported applications with the requisite experience to test software, hardware, and knowledge-based rules.

4.9.6 Develop test plans, schedules and procedures based on system performance specifications, policy and user requirements with each fielded RAPIDS release to supporting applications as directed by DMDC. Coordinate test site selection, preparation, software and/or hardware installation and testing at production facilities.

4.9.7 Determine statistical data collection requirements according to the change release scope required to assess and analyze system performance.

4.9.8 Collect test data and maintain test logs and error reporting according to DMDC procedures as identified in the RAPIDS Beta Testing Standard Operating Procedures (SOP) document.

4.9.9 Track error reporting, resolution and software changes pertaining to each test. *For informational purposes only:* Historically no more than four major and two minor RAPIDS releases were tested in addition to multiple hardware peripherals and one web application were tested in a given year, but this may not be indicative of future work.

4.9.10 Provide functional and technical expertise to review software and hardware training materials. Maintain an accurate log of the functional readiness of each application suite. Log Helpdesk tickets for non-functional equipment supported by the hardware vendor in the field environment.

4.9.11 Test all components of a system upgrade to include the hardware and software installation and training instructions designed for application self-service usage.

4.9.12 Moderate weekly user group teleconferences during test cycles; prepare and distribute meeting agenda and minutes. Provide weekly status information on products in beta test or preparing to be delivered for test.

4.9.13 Provide final test analysis and report to the Government required to make a production deployment decision within 5 work days of test conclusion but no later than two days prior to a production decision meeting.

4.9.14 Maintain historical test data in a shared library including but not limited to plans, issue logs, test cycle statistics (content, frequency, duration, etc.) for all test events using DMDC approved data collaboration tools.

4.9.15 Testing and evaluation support will be conducted on site at, but not limited to, DMDC's Mark Center facility. Remote access to the DMDC-housed RAPIDS application and hardware platform is not feasible.

4.9.16 Maintain and update technical specifications for COTS hardware requirements as system changes occur for operationally fielded systems such as RAPIDS, DBIDS, JAMMS and NTS, as well as for DMDC enterprise operations. See Appendix I

4.9.17 Track and coordinate the completion of the required testing and integration and report status to DMDC management through implementation.

4.9.18 Coordinate the enterprise and program-specific hardware planning monthly meetings and provide minutes following each meeting.

4.9.19 Assist with the life-cycle support of hardware, software, and telecommunications management, from defining technical requirements for products and equipment, monitoring platform/infrastructure integration and testing through implementation. The list of hardware and software supporting RAPIDS and DBIDS is shown in Appendix F and G respectively.

4.9.20 Assist the Government in developing and/or reviewing documentation, user guidance, hardware and software instructional materials, migration plans, etc.

4.9.21 Perform preliminary technical reviews and assessments of baseline documentation, System Requirements, Change Requests, Concept of Operations, Technical Reports, Test Plans, Test Cases, and Test Reports.

4.10 Contract Management – FFP

4.10.1 Plan, execute, and manage the work described in this PWS, employing DoD and DMDC policies, procedures, standards, guidelines, and industry best practices for project and program management; to include standards and methodologies published by the Project Management Institute (PMI) or other equivalent industry practices.

4.10.2 Create, update, and maintain a Contractor Program Management Plan (CPMP) that describes the approach, assessment processes to quantitatively measure performance organization, schedule, personnel and deliverables projected to meet the requirements of the PWS. The plan will include major milestones and dates on which they occur, dependencies and indications of critical path. The Contractor shall brief the final version of the management plan within thirty (30) calendar days of contract issuance, and return it to the Government five (5) working days after receipt of comments. The plan will also be maintained and updated for the life of the contract to reflect any significant changes in priorities, resource availability, tasks, or execution of the contract.

4.10.3 Submit a MSR for the previous month to the Contracting Officer Representative (COR) and a designated area in SharePoint by the 15th of each month. If the 15th falls on a weekend or holiday, the due date is automatically waived to the first workday following the weekend/holiday. The Contractor shall prepare an agenda and meeting summary in a clear, concise and orderly manner. Briefing materials shall be made available to all attendees prior to time of briefing. The report should include data of sufficient detail to monitor the completion of work products against progress as documented in the PWS: Order Summary, Performance metrics, Schedule, up to date Project Plan, Milestones achieved or missed, Open Issues/Risk and mitigation Action, Summary of Issues Closed, Projected Activities, Summary of accomplishments for each project.

4.10.4 Develop and deliver a Communications plan that provides methods, timing, roles, responsibilities and key messages. The Communication Plan will describe how the contractor will establish a reliable means of communicating status about the order 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.

4.10.5 The contractor shall be responsible for bringing to the attention of the COR any problems or potential problems in performing assigned tasks. Subsequent to verbal notification, a written Problem Notification Report (PNR) shall be submitted within three calendar days after identification of the problem.

4.10.6 The Contractor shall provide the Government with a Trip Report five (5) days after the travel is completed. The contractor shall identify the travel, to include: the name of the employee, location of travel, duration of trip, POC at travel location, task that the travel supports, benefit to the Government, accomplishments/lessons learned, and itemized listing of expenses, both planned and actual.

4.10.7 Provide a plan for transitioning out upon completion of the order. The Transition-Out Plan shall be due 60 calendar days prior to the end of the period of performance. Upon Government approval, the contractor shall implement its Transition-Out Plan. Prior to the end of the period of performance on this award the contractor shall begin to transition all data, information, training materials, deliverables, etc. required to perform the tasks in the PWS to the designated office (either Government or contractor).

4.10.8 Assist in facilitating meetings and activities associated with the transition planning and implementation of incoming programs.

4.10.9 Conduct a Post-Award Conference. 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 Post Award Conference 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 Post-Award Conference.

4.11 Surge Support (Optional)

The Government reserves the unilateral right to exercise Optional Surge Capability to support unforeseen, ad hoc requirements or unplanned increases in workload that may arise under the scope of this PWS. Optional surge capability support will be invoked at the Government's discretion through a written task order modification issued by the GSA Contracting Officer.

For pricing purposes, the Not-To-Exceed (NTE) ceiling amount established for this Optional Surge Capability in each year of performance is shown in the table below:

Base Year NTE	OY1 NTE	OY2 NTE	OY3 NTE	OY4 NTE
$1,500,000	$1,500,000	$1,500,000	$1,500,000	$1,500,000

Prior to awarding the modification, the Contracting Officer will provide the Contractor with a written request for surge capability specifying the unforeseen, ad hoc or unplanned increases in workload support required, the nature of work to be performed, deliverables, and required timeframes. The Contractor shall respond to this request in writing within five (5) business days with a quote showing the proposed staffing plan and notional schedule to meet the government's requirements. Generally, the Contractor shall have the capability to surge contractor staff to meet mission demands within 30 calendar days of the effective date of the modification. The Contractor shall manage workload surges effectively and in a manner that efficiently schedules and applies contractor resources to meet mission requirements and DMDC priorities. The Contractor shall meet the surge capability requirements without decreasing the current support to, or quality of, any of the other DMDC requirements under this task order.

The Contractor shall coordinate with the Government to plan and adjust staffing schedules to support surge capability activities while concurrently delivering ongoing services, without degradation, for day-to-day operations under the scope of this PWS. This may include adjusting normal work schedules, backfilling positions, or minimizing/prohibiting leave of individual Contractor employees to achieve the required coverage.

5.0 DELIVERABLES

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 contractor shall submit deliverables to the COR or his or her designee. The COR will serve as DMDC's focal point for accepting the deliverables. The general quality measures, set forth below, will be applied to each deliverable received from the contractor.

- 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.

The Government will provide written acceptance, comments and/or change requests, if any, within fifteen (15) 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 Reference	Due Date
Post-Award Conference	4.10.9	Within 5 days of award
Technology Roadmap	4.1.1.2	90 days after award; review annually; update ad hoc
Portfolio Human Capital Plan analysis and roadmap	4.1.1.8	90 days after award
Meeting Agendas, Summaries, Minutes, Action Items	4.1.1.5 4.2.1 4.4.13 4.4.15 4.4.16 4.4.19 4.6.1.2 4.8.1 4.9.12 4.9.18	Within 3 business day of the meeting/teleconference
Portfolio and Investment Strategic Calendar	4.2.1.1	Within 60 days of award; maintain and update quarterly thereafter

Cost / Benefit Analysis	4.2.2.2	Ongoing, as requested
Cost estimates	4.2.5.3	Ongoing, as requested
HRM Functional Strategy	4.2.8	Per the Project Management Plan
Integrated Master Schedule	4.3.3	Submitted 14 days after award and updated weekly
COTS acceptance packages	4.3.4.13	Within 5 business days of receipt of the ECP
Congressional responses, briefings and reports	4.4 4.8.2	Ongoing, as requested
Program Status and Performance Reports	4.4.5 4.4.19	Monthly
In-progress Reviews	4.4.5.1	Per the Portfolio and Investment Strategic Calendar, read-ahead due 5 days in advance
Risk Register	4.4.6	Ongoing
Program Strategic Communications Plan	4.4.17	Draft submitted 10 days of request; Final submitted within fifteen (15) days
Investment Resource Plan	4.5.3	Per the Project Management Plan
Milestone Decision Reviews	4.5.6	Per the Project Management Plan
Business Systems Design Specifications	4.5.6	Per the Project Management Plan
Update Standard Operating Procedures	4.3.2 4.4.4.2 4.6.1 4.8.5 4.9.8	Within 30 days of receipt of request and updated within 14 days of change request
SharePoint sites	4.6.3	Updated 14 days after award and updated within 3 days after documents change
Strategic Management Dashboards	4.6.8	Monthly
Master Data Management Standards document, Business Glossary, Data Lineage Repository	4.8.3	Standards Document – End of Base Year Business Glossary/Data Lineage Repository – 20% completed per year
Metadata Tagging Standards document, Metadata tags	4.8.4	Metadata Tagging Standards – Six Months after date of award

documented in Business Glossary		Metadata Tags Documented in Business Glossary – 20% completed per year
Standards documents for Data Access and Data Exchange	4.8.6	Nine months after date of award
MDM & Data Governance Cloud Migration Business Case and Roadmaps	4.8.7	End of Base Year
Set-up and data load into COTS MDM product	4.8.8	Per the Project Management Plan
Customer Agreements	4.8.1	Reviewed annually; new and updated agreements drafted within 10 days of requests
Test and Evaluation Plan	4.9.6	45 calendar days after award; with each fielded Operational System Release.
Final Test and Evaluation Report	4.9.13	No less than 2 business days prior to a scheduled production decision meeting.
Technical Specifications for DMDC Systems	4.9.16	Ongoing, as technology changes or new products are required
Contractor Program Management Plan	4.10.2	Draft submitted 15 days after award; Final submitted within fifteen (15) days after Draft and again at the exercise of a period of performance.
Monthly Status Report (MSR)	4.10.3	MSR brief shall be held on the fifteenth (15) calendar day of each month; electronic copy of the MSR shall be delivered 3 days prior to the brief
Contract Communication Plan	4.10.4	30 days after award
Problem Notification Report	4.10.5	3 days after identification of problem
Trip Reports	4.10.6	5 days after completion of travel
Transition Out Plan	4.10.7	60 work days prior to end of period of performance
Quality Control Plan	5.1	Draft submitted 15 days after award and final 30 days after award
Contract Risk Management Plan	5.3	Draft submitted 15 days after award and final 30 days after award
Organizational Conflict of Interest Mitigation Plan	5.4	Draft submitted with Quote and final 30 days after award; update as required

Non-Disclosure Agreements	5.5	Prior to any contractor personnel reporting for work
Annual Telework Report	5.12	Annually at end of each calendar year
CAC Status Report	7.2.1.8	Monthly

5.1 Quality Control Plan (QCP)

5.1.1 Establish a quality element that ensures compliance with applicable Federal mandates, contractual 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.

5.1.2 Maintain a thorough quality control program with the aim of identifying and correcting deficiencies in the quality of services before performance becomes unacceptable. Develop a Quality Control Plan (QCP) that describes the Contractor's procedures for monitoring performance. The COR will notify the Contractor, in writing, of deficiencies in the plan and allow 5 working days for a revision to be submitted.

5.1.2.1 Quality Status Reports (QSRs) shall be generated on a monthly basis. Details of audits and inspections accomplished, significant deficiencies noted, trend analysis of order performance and current status of all issues yet to be resolved. QSRs shall be distributed to the contractor's program management and Government representatives concurrently. At a minimum, the QSRs must include metrics, which verify whether the performance standards in the PWS have been met.

5.1.2.2 The quality control function shall ensure that timely and effective corrective action is obtained for all deficiencies identified by the Government.

5.1.2.3 The contractor may be required to conduct special inspections at the contracting officer's representative written request. Results of the inspection or audit shall be provided, in writing, in a timely manner as determined by the COR.

5.1.2.4 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.

5.2 Performance Standards

Performance Standard	Acceptable Quality Level (AQL)	Method of Surveillance
Delivery dates are met, or exceeded	99% are submitted on time	100% inspection

Deliverables are complete and accurate	95% correct the first time submitted	100% inspection
Project Management Plan	100% of areas required by government including the WBS are created and updated monthly. 95% On time delivery of Initial and Monthly Updates	100% Inspection
Quality Control Plan	95% compliance with Quality Control Plan	Random Monitoring and Partial Inspection Quarterly by COR
Risk Management Plan (RMP) RMP delivered on-time and updated monthly	100% on time delivery of initial RMP 95% delivery of updates by last workday of each month.	Routine inspection of deliverable products and services.
Support Service Staffing: Personnel possess necessary knowledge, skills, and abilities to perform tasks in accordance with the PWS and the kill set of the labor category quoted and accepted at call order award	Satisfactory or higher	CPARS/COR Observation/Customer assessments
Responsiveness	Responds to staff and acknowledges inquiry within one business day 99% of all inquiries are responded to within one business day	Direct Observation

5.2.1 Customer Complaint Surveillance. This action is instituted when the COR receives a complaint from a stakeholder 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 Contracting Officer and the complainant of the Government's response to their complaint.

5.2.2 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.

5.3 Risk Management Plan

The Contractor shall assess, evaluate, document, and manage risks associated with the performance of this order and create, modify, maintain, and implement a Risk Management Plan.

5.4 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.

5.5 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 Call Order 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 call order and whenever replacement personnel are proposed under an ongoing call order. Any information obtained or provided in the performance of this contract is only to be used in the performance of the call 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/Call Order performance.

5.6 Records/Data

The Government will be sole owner of all technical data, reports, and products produced under this project. The contractor shall deliver to DMDC all written documents and reports to include, at a

minimum, 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 task order. DMDC will have unlimited rights as allocated under FAR 52.227-14(b) in all data delivered under this order. 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.

5.7 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.

5.8 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.

5.9 Contractor Identification

All contract 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 in the minds of members of the public that they are Government officials. Electronic mail signature blocks shall identify contractor/company affiliation. They 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 staff 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, the contractor 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.

5.10 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 Contracting Officer's Representative (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.

5.11 Training Requirements for Government Contractors (5 CFR 930.301(1))

If contractors use Government computers, they shall complete DMDC sponsored IT Security Awareness training. The contractor shall track and report on training compliance. Completed certificates should be uploaded on SharePoint. Other DMDC mandated training courses include:

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

5.12 Teleworking

5.12.1 The Government may permit teleworking 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 teleworking agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Teleworking 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 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 prior to commencement.
- Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment
- 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

5.12.2 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. Time teleworkers spend in travel to the office should be tracked separately.

5.12.3 The Contractor shall establish a continuity of operation plan to telework in the event Government offices are closed due to a contingency

5.13 Key Personnel

Key personnel are considered essential to successful contractor performance. All key personnel shall be available for work under this contract from the date of contract award. Furthermore, key personnel shall be available for the entire period of performance of this contract. If it should become necessary to substitute or replace Key Personnel, the contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement Key Personnel within 14 calendar days of the notification. The notice shall provide a detailed explanation of the circumstances necessitating the substitution. Qualifications of substitute personnel shall be equal to, or greater than, the requirements specified within this document. The candidates shall be available to begin performance within 14 calendar days of Government concurrence.

The following Key Positions have been identified for this contract:

- Program Manager (Site Lead)
- Senior Subject Matter Expert (Patient Identity)
- Senior Subject Matter Expert (Identity, Credential, and Access Management)
- Systems Engineer (support for RAPIDS)

Program Manager (Site Lead) Criteria Required:

- 7 years of DoD program management experience on enterprise IT applications including both COTS and GOTS systems with cost, schedule and performance responsibilities for an enterprise system
- DAU Program Management Certification (Level 3) with focus on Services and/or Business Systems Management/IT *(or commercially available equivalent certification and at least 7 years of experience with federal programs)*

Patient Identity SME Criteria Required:

- 10 years of experience in the Patient Identity domain with 5 of which within DoD
- 3 years of experience with Federal Interoperability with VA
- 5 years of experience with Defense Health program/financial management
- 3 years of experience with Defense Health focused on Enterprise Systems

Desired:

- Knowledge and experience with Cerner Millennium and Healthy Intent

Identity, Credential, and Access Management SME Criteria Required:

- 10 years of experience in the Identity and Access Management domain with 5 of which within DoD
- Demonstrated knowledge and experience applying HSPD 12
- Demonstrated knowledge and experience applying NIST Standards for IDAM
- 5 years of experience with Federal Interoperability preferably with VA (can be concurrent with other requirements)
- 3 years of demonstrated expertise with DoD policy and package coordination with the P&R front office and DoD CIO (can be concurrent with other requirements)

Desired:

- Knowledge of market offerings and application of second factor authentication alternatives
- 2 years of demonstrated expertise with federal and DoD governance bodies for identity (Can be concurrent with other requirements)
- CISM or CISSP Credentials

Systems Engineering (RAPIDS) Support Criteria Required:

- 5 years of experience researching industry technologies and engineering solutions for emerging COTS hardware and software; technically evaluating COTS hardware and software products for integration into complex desktop applications requiring biometric capture and credentialing solution integration; conducting and documenting analyses of alternatives.
- 3 years of proficiency analyzing Federal and DoD technical and cyber security regulations and requirements for hardware and software and applying knowledge to product evaluation for integration into multiple worldwide DoD desktop and laptop products.
- 3 years of experience in hardware/software lifecycle planning; managing enterprise-wide hardware test, selection and integration processes to ensure mandatory equipment is fielded without service interruption.
- In-depth knowledge and experience of identity management COTS hardware, software, and technical requirements and regulations.

Desired:

- Experience and participation in engineering change proposal processes.
- Knowledge of Federal and DoD Public Key Infrastructure technical requirements pertaining to COTS hardware and software.

6.0 ADMINISTRATIVE CONSIDERATIONS

6.1 Hours of Work / Place of Performance

The contractor is responsible for conducting business, between the hours of 8 a.m. to 5 p.m., 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 performed under this task will be performed largely on site at DMDC facilities in Monterey California, and the Mark Center, Alexandria, Virginia. The RAPIDS beta test lab is located in the Mark Center and all associated tasks shall be performed at the Mark Center. All Key Personnel are required to be on site. On-site personnel will follow OPM's operating status guidance. Any work performed at other locations must be identified in your technical quote and approved by the Government. Implementation and test management support may be required periodically during evenings and weekends to support customer implementations.

6.2 Period of Performance

The period of performance for this call order shall be one year from date of award plus four 12-month option periods. The Government shall have the unilateral right to exercise option periods in accordance with FAR Clause 52.217-9 Option to Extend the Term of the Contract:

1) 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.
2) If the government exercises an option, the extended contract shall be considered to include this option clause.
3) The total duration of this contract, including the exercise of any options under this clause, shall not exceed sixty (60) months; with the exception of any potential bridge of the contract for an emergency continuance of contract performance to be awarded for the benefit of the Government.

6.3 Travel

The Government anticipates that travel may be required during the performance period. Exact locations and frequency are unknown at this time. Specific locations, dates and personnel required, etc., shall be identified by DMDC during task performance. It is anticipated that trips will include travel to attend meetings and to support Data Management applications and projects.

The Not-To-Exceed dollar value established for Travel is $35,000.00 per each performance period. This Travel ceiling shall not be exceeded without the advanced written approval of the Contracting Officer.

All travel shall be pre-approved by the DMDC COR to ensure that funding and approvals are obtained before incurring any travel costs. Reimbursement shall include full travel costs and per diem reimbursement consistent with the Federal Travel Regulations, and reimbursement of general and administrative expense, as appropriate. Where feasible, the Contractor will use teleconferencing and electronic media transfers of data as much as possible to limit travel costs. The Contractor will seek the least expensive form of travel as is practical to the fulfillment of the performance of the contract.

In accordance with FAR 31.205-46, travel costs are to be reimbursed at rates not to exceed the maximum locality per diem rates (the combination of lodging, meals and incidentals) in effect at the time of travel, as set forth in the Federal Travel Regulations, Joint Travel Regulation and Standards

Regulations, Section 925, as applicable. All air travel must be booked on American flagged carriers, unless otherwise directed by the Contracting Officer. All invoices for travel reimbursement shall be accompanied by supporting receipts.

6.3.1. Travel Regulations

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

- Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.
- Joint Travel Regulations (JTR), Volume 2, Department of Defense (DOD) Civilian Personnel, Appendix A - prescribed by the DOD, for travel in Alaska, Hawaii, and outlying areas of the U.S.
- 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.

6.3.2 Travel Authorization Requests

Before undertaking travel, other than local to any contractor off-site location, to any Government site or any other site under this contract, the contractor shall have this travel approved by, and coordinated with, the DMDC COR. 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 Authorization Request for Government review and approval. The Travel Authorization Request shall:

- Be prepared in a legible manner
- Include a description of the travel proposed including a statement as to purpose
- Be summarized by traveler
- Identify the call order number
- Identify the CLIN associated with the travel
- Show the concurrence of the Government Program Manager who validated the required travel
- Be submitted in advance of the travel with sufficient time to permit review and approval
- Include: Name of each contractor employee and position title; a description of the travel proposed including a statement as to purpose; and the estimated cost.

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. Local travel from off-site locations shall be at the contractor's expense.

6.4 Government Furnished Equipment (GFE)

The Government will provide office supplies, and computer and software resources at DMDC Seaside, CA and the Mark Center, VA, if applicable. Off-site personnel will only be provided with VDI software to access DMDC's network. The contractor has the primary responsibility for exercising reasonable care and control of GFE in its possession, or usage. Responsibility for reasonable care and control of GFE provided under the call order in the possession of a subcontractor remains with the prime contractor.

The contractor may be liable for damages, shortages of GFE when it is disclosed that the equipment is lost, damaged, or destroyed. GFE must be used only for the purposes set forth in this call order.

Upon request of the Government, all Government furnished items shall be returned to the Government. All equipment or items furnished to the contractor shall be surveyed and a GFE/GFI list report shall be delivered to the COR at end of the call order.

6.5 Government Furnished Information (GFI)

The Government will provide the following information: access to relevant Government organizations, information and documentation, manuals, texts, briefs, and associated materials as required and available. Access will be granted to classified networks under the guidance of the appropriate Government Security Manager.

7.0 SECURITY

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 Common Access Card (CAC) and public trust position at the appropriate level or security clearance prior to the call order start date.

7.1. Security Clearance Requirements

Personnel performing on this PWS requiring access to classified information shall obtain a **Secret** clearance in accordance with the DD 254, Contract Security Classification Specification. The Contractor must possess or obtain a facility security clearance at the level of Secret prior to contract award. The Contractor shall register and request security clearances through the National Industrial Security Program Central Access Information Security System (NCAISS) (https://www.dss.mil/is/ncaiss/). Contractor personnel shall have appropriate clearances prior to contract award unless otherwise approved in writing by the Contracting Officer (CO). If subcontractors are utilized in performance of a classified contract, the Prime Contractor shall create a Subcontract DD 254 in the National Industrial Security Program Contract Classification System (NCCS). The Prime Contractor shall ensure that any teaming partners or subcontractors have the appropriate security clearances prior to contract award. 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.

7.1.2 DHRA is not responsible for processing contractor personnel for national security clearance (Secret and Top Secret).

7.1.3 The contractor must comply with required DEOC personnel security requirements as specified by the DHRA Enterprise Operations Center (DEOC).

7.1.4 Interim Clearances (e.g., Interim-Top Secret, Interim-Secret) will be reviewed by DEOC Security.

7.1.5 It is the responsibility of the contractor Facility Security Officer (FSO) to notify DEOC Security immediately if there is a change in clearance eligibility.

7.1.6 If at any time, any contractor person is unable to obtain/maintain an eligibility for access to classified information, the contractor FSO shall immediately notify DEOC and DMDC Cybersecurity Division and remove such person from work under this contract.

7.1.7 A SF 312 Non-Disclosure Agreement (NDA) initiated by the company's Facility Security Officer (FSO) is required for each of the Contractor's personnel.

7.2. CAC Requirements

7.2.1. 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 order:

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

7.2.1.2. Provide two forms of identity proofed identification (I-9 documents)

7.2.1.3. Be citizens of the United States

7.2.1.4. Submit a Tier 3 vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably adjudicated by the Defense Counterintelligence Security Agency (DCSA) for all employees under this contract requesting a position of trust determination for those::

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

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

7.2.1.7. 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.

7.2.1.8 The contractor will submit a monthly report identifying the CAC status of personnel. The report will identify if the employee has a CAC, the on-board date, the off-board date (if applicable), and if the employee has departed, the date the CAC was collected and by whom.

7.3. Position of Trust Requirements

7.3.1. All Contractor personnel with access to DMDC systems or data must comply with DODI 5200.2-R and DODI 8500.1. All persons on this contract will be designated as either an IT-I or IT-II as determined by the Government per position responsibilities. All enterprise wide system administration support, to include the mainframe support services will require IT-I. Prior to beginning work on this contract, the Contractor will complete all required DMDC personnel security requirements as specified by the Cybersecurity Branch.

7.3.2 Submit a Tier 3 vetting application (Standard Form (SF) 86 National Security Questionnaire through e-QIP, fingerprints and proof of US citizenship) that is favorably adjudicated by the Defense Counterintelligence Security Agency (DCSA) for all employees under this contract requesting a position of trust determination.It is the responsibility of the Contractor to ensure their employees and sub-Contractors (if applicable) comply with DMDC personnel security requirements.

7.3.3 Listing of Employees & Clearance Documentation. The Contractor shall maintain a current listing of employees. Within 10 calendar days of contract award, the Contractor shall provide the COR a list with the names, location of performance and clearance requirements of all company employees assigned to this effort. The list shall be validated and signed by the company DHRA Personnel Security. An updated listing shall be provided when an employee's status or information changes.

7.3.4 Controlled/Restricted Areas. The Contractor shall be compliant with local procedures for entry to DHRA controlled/restricted areas where Contractor personnel will work.

7.3.5 Physical Security. The Contractor shall safeguard all Government property and controlled forms provided for Contractor use and adhere to the Government property requirements contained in this contract. At the end of each work day, all Government facilities, equipment and materials shall be secured.

7.3.6 Pass and Identification Items. The Contractor shall ensure the pass and identification items required for contract performance are obtained for employees and non-government owned vehicles.

7.3.7 Personnel must be citizens of the United States.

7.3.8 Retrieving Identification Media. The Contractor shall retrieve all identification media, including vehicle passes from employees who depart for any reason before the contract expires; e.g. terminated for cause, retirement, etc.

7.3.9 Weapons, Firearms, and Ammunition. Contractor employees are prohibited from possessing weapons, firearms, or ammunition, on themselves or within their contractor-owned vehicle or privately-owned vehicle while on all DHRA installations.

7.3.10 Controlled Unclassified Information Requirements for DoD Contractors. The following procedures will be used to protect Controlled Unclassified Information (CUI) documents and materials:

7.3.10.1 HANDLING: Access to CUI material shall be limited to those employees needing the material to perform their duties. The CUI marking is assigned to documents and material created by a DoD User Agency. CUI is not a classification, but requires extra precautions to ensure it properly safeguarded and disseminated and is not released to the public without government authorization.

7.3.10.2 MARKING: Mark unclassified documents containing CUI: “CUI" at the top and bottom of each page, include the CUI warning box, and the CUI Designation Indicator Block as required in DoDI 5200.48. In a classified document:

7.3.10.2.1 Mark individual paragraph containing only CUI, but not classified material by placing “(CUI)" at the beginning of the portion.

7.3.10.2.2 Mark top and bottom of each page with classified material with the highest security classification of the material on the page.

7.3.10.2.3 If the document or material contains CUI under the category of Controlled Technical Information (CTI), use of distribution statements is required. See DoDI 5200.48.

7.3.10.2.4 If a classified document contains CUI material or if the classified material becomes CUI when declassified, place the following statement on the bottom of the cover or the first page under the

classification marking: “NOTE: If declassified, review the document to make sure the material is not still CUI. If it does, then it must have the appropriate safeguarding, dissemination controls, and CUI markings applied.

7.3.10.2.5 Mark other records such as computer print outs, photographs, films, tapes, or slides in accordance with DoDI 5200.48 so the receiver or viewer knows the it contains CUI material.

7.3.10.2.6 Mark a message containing material in accordance with DoDI 5200.48. Unclassified messages containing CUI material must show the abbreviation (CUI) before the text begins.

7.3.10.2.7 Ensure documents transmitting CUI material call attention to any attachments containing CUI.

7.3.10.2.8 CUI material released to a contractor by a DoD user agency must have the following statement on the front page or cover:

THIS DOCUMENT CONTAINS CUI MATERIAL AND MUST BE REVIEWED BY A GOVERNMENT REPRESENTATIVE UNDER THE REQUIREMENTS OF DODI 5200.48, DODI 5230.09, and DODI 5230.29.

7.3.10.3 STORAGE: During normal duty hours, place CUI material in an out-of-sight location if your work area is accessible to persons who do not have an authorized government purpose for access to the material. After normal duty hours, store CUI material to prevent unauthorized access. File with other unclassified records in unlocked files or desks when internal building security is provided and the file is marked as CUI. When there is no internal security, locked buildings or rooms usually provide adequate after hours protection. For additional protection, store CUI material in locked containers such as file cabinets, desks, or bookcases. Expenditure of funds for security containers or closed areas solely for the protection of CUI material is prohibited.

7.3.10.4 TRANSMISSION: CUI documents and materials may be transmitted via first class mail, parcel post or for bulky shipments-fourth class mail. Within the CONUS discussion of CUI material on the telephone is authorized if necessary for the performance of the contract and no alternative is available. Electronic transmission of CUI (voice, data, or facsimile) should be by approved secure communications systems whenever practical. If there is a fax transmission, the sender must ensure the intended receiver is available to receive it or a cover sheet will be used to allow carrying it to the final recipient to avoid unauthorized disclosure of the CUI.

7.3.10.5 RELEASE: CUI material shall not be released outside of the contractor’s facility except to the representative of DoD or DHRA.

7.3.10.6 DESTRUCTION: When the CUI material no longer meets the threshold for safeguarding and dissemination, it shall be immediately decontrolled, be processed through the records management process, and destroyed by the approved methods identified in DoDI 5200.48 precluding its disclosure to unauthorized individuals by rendering it unreadable, indecipherable, and irrecoverable.

7.3.11 Reporting Requirements. Contractor personnel shall report to an appropriate authority any information or circumstances of which they are aware may pose a threat to the security of DOD personnel, Contractor personnel, resources, and classified or unclassified defense information.

7.3.12 Key Control/Access Badge Control. The Contractor shall establish and implement methods of making sure all keys/badges issued to the Contractor by the Government are not lost or misplaced and

are not used by unauthorized persons. The Contractor shall not duplicate any keys issued by the Government.

7.3.12.1 Prohibited Use. The Contractor shall prohibit the use of keys, issued by the Government, by any persons other than the Contractor's employees and the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in performance of contract work requirements in those areas.

7.3.13 Lock Combinations. The Contractor shall control access to all government provided lock combinations to preclude unauthorized entry. The Contractor is not authorized to record lock combinations without written approval by the COR. Records with written combinations to authorized secure storage containers, secure storage rooms, or certified vaults, shall be marked and safeguarded at the highest classification level as the classified material maintained inside the approved containers.

7.3.14 Government Furnished Equipment (GFE). The Contractor shall establish and implement procedures to ensure all GFE to include laptops and other data processing devices, issued to the Contractor by the Government are not lost or misplaced, are not used by unauthorized persons or are not subject to unauthorized external devices. The Contractor shall immediately report to the COR any occurrences of lost GFE within two (2) hours of discovery of occurrence. In the event that GFE is lost, the Contractor may be required, upon written direction of the CO, to replace the equipment at no additional cost to the Government. The Government may replace the equipment and deduct the cost of such from the monthly payment due the Contractor.

7.3.15 Conduct while on Government Installation. The CO may direct the contractor to remove an employee(s) from an assignment under this contract for reasons of security or misconduct. Where the reasons for the removal request is due solely for security or misconduct by the employee(s), the replacement shall be at the contractor's expense and not chargeable to the government.

7.4 LAN Access Requirements

The Contractor shall comply with account access requirements as specified by the DMDC Cybersecurity 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).

7.5 Information Assurance Requirements

7.5.1. 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 Cybersecurity, DODI 8510.01 Risk Management Framework, NIST 800-53, 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.

7.5.2. 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 DoDD 8500.01 and DoDI 8510.01 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

7.5.3. 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 and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to RMF must present evidence of Assessment and Accreditation (A&A). Evidence of FISMA compliance must be presented in the form of a POA&M. The Contractor will be responsible for the cost of IA A&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

7.5.4 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.

7.5.5 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.

7.5.6 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 organization directly concerned with the performance of the contract.

7.5.7 The contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the COR and corrective actions will be implemented immediately.

7.5.8 Cyber Incident Reporting. Within one (1) hour of discovery of any cyber incident the Contractor shall notify the DMDC Incident Response (IR) team by emailing an Initial cyber incident report to the following organizational box: dodhra.dodc-mb.dmdc.list.ir-team@mail.mil , with subsequent reporting every 24 hours until the incident is closed.

7.5.9 The contractor will 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.

7.5.10 Compliance with Cybersecurity and Privacy DoD Instructions and Directives. The Contractor and all Contractor personnel with access to or responsibility for nonpublic Government data under this contract shall be in compliance with the latest versions of:

DoD Instruction (DoDI) 8500.01, Cybersecurity
DoD Instruction (DoDI) 8510.01, DoD Risk Management Framework (RMF) for DoD Information Technology (IT)
The Privacy Act (5 U.S.C. 552a)
DoD 5400.11-R, and DoD Directive 5400.11, DoD Privacy Program
DoD 6025.18-R DoD Health Information Privacy Regulation
DoD 5200.2-R, Personnel Security Program
HSPD-12, Homeland Security Presidential Directive
NIST SP 800-137, Information Security Continuous Monitoring
DODI 8140, Cybersecurity Workforce
DOD 8570.01-M, Information Assurance Workforce Improvement Program

7.5.11 Cyberspace Workforce Management Requirements. The Cybersecurity Workforce includes, but is not limited to, all individuals performing any of the cybersecurity functions described in DOD 8570.01-M. The cybersecurity workforce must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened in accordance with DOD 8140.01 and supporting issuances. It is imperative to the DHRA mission that the cybersecurity workforce establish baseline technical and management cybersecurity skills among personnel performing cybersecurity functions across the DHRA enterprise. The Contractor shall ensure information assurance workforce personnel have appropriate qualifications in accordance with DoD 8570.01-m prior to contract award.

7.5.11.1 Cybersecurity functions are focused on the development, operation, management, and enforcement of security capabilities for systems and networks. Personnel performing cybersecurity functions establish cybersecurity policies and implement security measures and procedures for DHRA and affiliated information systems and networks.

7.5.11.1.1 Cybersecurity measures to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.

7.5.11.1.2 Job functions that require privilege access to DHRA assets.

7.5.11.1.3 Cybersecurity duties may be performed as primary or additional/embedded duties, by a DHRA employee (civilian, military or contractor).

7.5.12 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.

7.5.13 The Contractor is responsible for safeguarding all Government equipment, information and property. At the close of each work period, Government facilities, equipment, and materials shall be secured.

7.6. Classified Data Processing

Based on DoD Regulation 5200.2-R, some aspects of the tasking described in this PWS requires, at minimum, a SECRET Clearance, or a SECRET Clearance In Progress, for employees who support the classified systems and/or applications at DMDC. All documentation and cost for clearance processing shall be the responsibility of the contractor. Upon award, a DD Form 254 will be issued to the

contractor. All classified data processing must be completed in an approved classified processing facility. Approved classified processing facilities include: DMDC, Seaside, CA, and the Mark Center, Alexandria, VA.

7.7 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.

8.0 INVOICE CLAUSE

Clause #1 - Invoices

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month *(for services)* or

(2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice shall show by task, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that

invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Note: For Firm Fixed Price, Labor Hour, and Time and Material fiscal task items:

Charges:

- All invoice charges must be task item specific (only one task item) unless concurrent task item periods of performance exist.

- For invoices with concurrent task item periods of performance all invoice charges must be service month specific (that is one service month only).

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, task item, 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
P.O. Box 6200-29

Portland, OR 97228-6200

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 COTR to electronically accept and certify services received by the customer representative (CR). Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following option 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.

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Interim close outs: The Government will close out each year of performance within 6 months of its expiration using the rates billed during that period. The contractor will be required to execute a waiver of claims to be included in a bi-lateral modification at the conclusion of the performance period.

Final Invoice: Invoices for the final performance period must be so identified and submitted within 6 months from completion. After this submission, no further charges are to be billed. A copy of the written client agency acceptance of task completion must be attached to the final invoice. If necessary, the contractor may request from GSA an extension for a final invoice that may exceed the 6-month time frame.

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.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary*.

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. 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.

Clause #2 - Acceptable Skill Level Variation in Severable Labor Hour and Time and Material Orders/Contracts (July/2005)

The contractor may exceed the total number of *labor* hours per *awarded* skill level per base or option period, to a limit of 15% as long as the total task order *obligated* dollar amount per that base or option period is not exceeded, and *as* long as the contractor maintains an acceptable level of effort throughout the required period of performance.

The contractor is not authorized to add new skill level categories or vary between levels within the same labor category without approval of the Government, formalized in a signed modification by the contracting officer.

FAR 52.209-11: Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Feb 2016)

(a) As required by sections 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that–

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and

made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that–

(1) It is __ is not __ a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) It is __ is not __ a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

DFARS 252.232-7007, LIMITATION OF GOVERNMENT'S OBLIGATION (APR 2014)

(a) Contract line item(s) *[Contracting Officer insert after negotiations]* is/are incrementally funded. For this/these item(s), the sum of $ *[Contracting Officer insert after negotiations]* of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph (j) of this clause.

(b) For item(s) identified in paragraph (a) of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).

(c) Notwithstanding the dates specified in the allotment schedule in paragraph (j) of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph (j) of this clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph (j) of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will

terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled “Termination for Convenience of the Government.”

(d) When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph (a) of this clause, the parties will agree as to the period of contract performance which will be covered by the funds. The provisions of paragraphs (b) through (d) of this clause will apply in like manner to the additional allotted funds and agreed substitute date, and the contract will be modified accordingly.

(e) If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph (a) of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled “Disputes.”

(f) The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph (a) of this clause.

(g) The termination provisions of this clause do not limit the rights of the Government under the clause entitled “Default.” The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph (a) of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraphs (d) and (e) of this clause.

(h) Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled “Termination for Convenience of the Government.”

(i) Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

(j) The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

On execution of contract	$ _____
(month) (day), (year)	$ _____
(month) (day), (year)	$ _____

(month) (day), (year)	$ _____

(End of clause)

252.239-7001: INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)

(a) The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including—

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

(b) Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

(c) Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

(End of clause)

9.0 APPENDIX

A. DMDC Strategic Management Plan

B. Historical Information

C. RAPIDS Beta Test Report Sample

D. RAPIDS Beta Test Matrix Sample

E. RAPIDS Beta Test Log Sample

F. RAPIDS Fielded COTS Hardware

G. DBIDS Hardware Equipment List

H. DMDC COTS Acceptance Test Methodology and Process

I. Hardware and Software Technical Specifications

J. Business Processes Approved Handbooks

K. Key Personnel Requirements

L. DHRA Zero Trust Implementation Plan

M. DoD Zero Trust Reference Architecture

N. DoD Enterprise Identity, Credential, and Access Management (ICAM)