PERFORMANCE WORK STATEMENT

Missile Defense Agency Information Technology & Engineering Solutions (MIOES)

Contract Number: TBD

ENTERPRISE IT SERVICES AND SERVICE DELIVERY

Task Order Number: F-8000

Period of Performance: TBD

MIOES Task Order 2- Enterprise Services and Service Delivery

1.0 Background

The Office of the CIO is responsible for providing Information Technology (IT) Governance across the Missile Defense Agency, this includes but is not limited to establishing the policies for the procurement and acquisition of information technology products and services and the management of IT projects servicing agency stakeholders and customers. IC is responsible for customer outreach, execution, management and oversight of the CIO's portfolio of enterprise assets and acquired services.

2.0 Scope

Task Order 2 enables IT services critical to the agency CIO's mission to confirm that IT services and resources are administered, acquired, managed, operated, and cyber defended in compliance with the goals and directives of existing statutes and DoD regulations and the priorities set by the MDA Director and CIO. The primary scope of this PWS encompasses Portfolio Management, Planning and Integration, Architecture and Engineering, Network Operations, End User Services and Service Delivery. The key for successful execution of the MIOES contract is the understanding that all Task Orders are to be fully integrated and aligned. Any modifications to any Task Order must be fully vetted across all Task Orders to reduce; potential risks, cause interruption of services or delays, duplicative efforts, or otherwise negatively impact the agency.

3.0 Contract Data Requirements List (CDRL)

The point of delivery for all CDRL products, except as noted in Exhibit C, is the Electronic Content and Records Tool (E-CaRT) system. The contractor shall deliver all such products by saving and profiling them in E-CaRT, with the appropriate notification of delivery letter transmitted electronically to the Government's Data Management Office (DMO). Reference Exhibit C for specific CDRL delivery instructions.

Task	CDRL	DID	Title
8.2.1.3	A001	DI-MISC-80368A/T	Status Report, [Month Ending]
8.2.2.2	A002	DI-MGMT-81861C	Integrated Program Management Data and Analysis Report (IPMDR) (Schedule Only) (For FFP tasks)
8.2.2.2	A003	DI-MGMT-81861C	Integrated Program Management Data and Analysis Report (IPMDR) (Full) (For CPIF tasks)
8.2.3.1	A004	DI-MGMT-81453A	Data Accession List (DAL)
8.2.4.1	A005	DI-MISC-80508B/T	Task Order Close-Out
10.5	A006	DI-MISC-80508B/T	Lifecycle Plan
8.6	A007	DI-MISC-80508B/T	COOP-DR Testing and Training Plan

8.6	A008	DI-MISC-80508B/T	Disaster Recovery Plan and Incident Response Plan
9.2	A009	DI-MISC-80508B/T	Service Portfolio Management Strategy Plan
10.3	A010	DI-MISC-80508B/T	Customer Relations Management (CRM) Plan
10.6	A011	DI-MISC-80508B/T	Configuration and Change Management Plan
10.7.1	A012	DI-MISC-80508B/T	Information Technology Updates and Refreshment Strategy

4.0 Service Summary Items

- TBD

5.0 Government Property

The contractor is required to be in compliance with FAR 52.245-1, Government Property. The Logistics and Product Services task order under the MIOES contract will provide the following integrated service capabilities and requirements for all task orders under this contract: warehouse operations, inspection, shipping, receiving, tagging, cataloging, packaging, handling, storage, transportation (local and third party) and life cycle property management from receipt, periodic inventories to disposal operations. All other activities required to be in compliance with FAR 52.245-1, shall be performed under this task order and will be adhere to the property management, asset management and accountability requirements as specified within the MOES Property Management and Logistics Services Task Order.

6.0 Other Requirements

None

7.0 Other Issuances

In addition to the issuances identified in the Contract, the following are applicable to this task order:

Document ID	Title	Originator	Date
TBD			
TBD			

8.0 Performance Objectives and Standards

8.1 Contract Level Management (CPFF)

Reference Basic PWS 8.1

8.2 Task Order Management (CPFF)

8.2.1 Task Order Program Management and Leadership

The contractor shall provide task order (TO) level program management and leadership ensuring execution, oversight, and administration of all TO requirements within the integrated framework of the contract. The contractor shall monitor performance, manage risks, and provide quality deliverables, adhering to DoD and Agency standards.

Standards:

8.2.1.1 Lead, manage, and execute TO activities in accordance with the MIOES Program Management Plan.

8.2.1.2 Manage technical, cost, and schedule performance and associated risks and provide updates at the Risk Review Boards.

8.2.1.3 Provide situational awareness by reporting on items such as the following: Status of technical, cost, and schedule performance, significant accomplishments and customer concerns, TO risks, mitigation, and remediation status, performance trends and progress against Quality Assurance Surveillance Plan (QASP) metrics. (CDRL A001)

8.2.1.4 Operate within and follow the contract wide processes and governance models in executing systems engineering, mission assurance, quality assurance, configuration management requirements outlined in the PWS.

8.2.1.5 Participate in and deliver Integrated Product Team artifacts in preparation of TO modifications and follow-on TOs

8.2.1.6 Develop and deliver proposals in accordance with the RFP letter from the PCO, for TO modifications and follow-on task orders

8.2.1.7 Prepare for and participate in audits, such as Inspector General, IT security, cyber security, physical security, GAO, property, environmental, health and safety.

8.2.1.8 Comply with export control requirements (e.g., ITAR, 22 CFR 120-130) and technical assistance agreements.

8.2.1.9 Comply with the MDA and MDIOC Facility Systems Engineering Plans (SEP)

8.2.1.10 Provide a cleared, cyber workforce certified IAW DoDM 8140.03, with all positions documented in the Cyber Workforce Qualifications Tracker (CWQT):

- Position Title, Description, and DoD Cyberspace Workforce Framework (DCWF) Cyber Code Alignment.
- Security Clearance, Sensitivity Level, and System Privilege Level.
- Verification and quarterly validation of contractor-filled roles in agency CWQT.

8.2.1.11 Lead, manage, and execute TO activities in accordance with the Cyber Resiliency Management Plan delivered under the Cybersecurity task order.

8.2.1.12 Develop a Cyber Workforce Training Plan for contractor personnel, aligning with the DoD Cyber Workforce Framework (DCWF).

8.2.1.13 Identify and recommend Artificial Intelligence and Automation (alternate solutions) when and where practical to gain efficiencies or cost reductions. Provide recommendations to the COTR in the monthly status reports.

8.2.1. 14 Leverage automation practices and tools where practical throughout the Task Order and report on automation practices in the monthly status report.

8.2.2 Task Order Measurement and Control

The contractor shall monitor, measure, control, and report contract cost, schedule, and performance metrics at the TO level.

Standards:

8.2.2.1 Implement and administer a compliant Earned Value Management System (EVMS)

8.2.2.2 Deliver the Integrated Program Management Data and Analysis Report (IPMDAR)

- Deliver an IPMDAR (schedule only) for FFP tasks. (CDRL A002)
- Deliver an IPMDAR (full) for CPIF tasks (CDRL A003)

8.2.2.3 Integrate the TO Integrated Master Schedule (IMS) into the MIOES Integrated Schedule (IIS) (IIS dictated in the IPMDAR)

8.2.2.4 Perform a Baseline Review or Integrated Baseline Review within 90 days of contract award for CPIF tasks.

8.2.2.6 Provide subcontracting and limitation of funds oversight, and execution of TO modifications and awards

8.2.2.7 Provide management, oversight and quality control for program control documentation, processes, and reports.

8.2.3 Data Accession List (TO Level)

The contractor shall provide a Data Accession List (DAL).

8.2.3.1 Deliver the DAL, providing a medium for identifying contractor internal data which has been generated. (CDRL A005)

8.2.3.2 Provide a document reference number for each DAL item for rapid retrieval from contractor data sources.

8.2.4 Task Order Close-Out

The contractor shall execute TO close out procedures, consolidate TO data, to provide seamless closeout of TO activities.

Standards:

- Perform a TO closeout that consolidates all TO data and deliver a Task Order Close-Out Report. (CDRL A006)

8.3 Security Administration

(Firm Fixed Price)

The contractor shall provide security administration IAW applicable DoD, Agency, and local security directives, classification guides, policies, procedures, and instructions in the safeguarding of controlled and classified information, including proper document marking, classification, storage, accountability, transmittal, and destruction.

Standards:

- Manage international security IAW DoD and Agency requirements (Foreign Disclosure [FD], ITAR, Trade Act Agreement [TAA]).
- Protect CPI and CT IAW DoDI 5200.39, Critical Program Information (CPI) Protection within the DoD.
- Execute security protections which include marking and Handling IAW DoDI 5200.01 Volumes 1-IV.

8.4 Monitoring and Reporting

(Firm Fixed Price)

The contractor shall provide continuous security and performance monitoring services for the infrastructure, including servers, networks, and applications. These services will support proactive threat detection, performance optimization, and compliance with DoD cybersecurity policies, including DISA STIGs, RMF, and NIST 800-53.

Standards:

- Operate a 24/7/365 Global Network Operations Security Center (GNOSC) to monitor, diagnose, and resolve network issues for government-identified CIO applications and services.
- Establish network baseline expectations and monitor performance properties for classified/unclassified systems, including latency, loss, jitter, throughput, bandwidth utilization, circuit degradation, and other government-provided indicators.
- Detect deviations from baseline parameters and institute automated alerts to provide consistent insights into network performance and provide notifications to monitoring personnel.
- Define trends to identify the source and nature of network performance reliability issues, including latency, response time, reliability, and alerts.
- Take corrective actions to restore network performance to approved baseline parameters and monitor reliability to mitigate vulnerabilities, such as Single Points of Failure (SPoFs).
- Provide warning notifications to the WAN Management Team per the COOP/DR plan, notifying the government within 30 minutes of:

    - Circuit utilization:
        - 50% (initial notification).
        - 80% (secondary notification).
        - Monthly updates to the COTR for consistent utilization above 80%.
    - Perceptible trends:
        - More than three outages in one month.
        - Six outages in three months.
    - Circuit degradation:
        - Circuits below 70% operational for one month.
- Submit status reports on circuit utilization, degradation, identified trends, and overall utilization, with updates until issues are resolved via dashboard.
- Conduct performance trend analysis to support capacity planning, regular testing to validate SLA compliance, and vulnerability scans per DoD timelines.
- Deliver key reports: weekly security monitoring, monthly performance monitoring, quarterly STIG checklists, and semi-annual configuration compliance via dashboard.
- Meet KPIs: MTTD ≤ 10 minutes, MTTR ≤ 4 hours, uptime ≥ 99.9%, and 100% compliance with DoD security directives.
- Maintain documentation of configurations, maintenance activities, and compliance audits, while documenting design and architecture changes per configuration management policies.

8.5 Incident Handling, Problem Management and Disaster Recovery

(Cost Plus Fixed Fee)

The contractor shall manage and resolve incidents and problems across the entire infrastructure. The includes incident detection, response, resolution, root cause analysis, and proactive problem management for all servers, applications, and networks, with a focus on mission-critical operations and compliance with DoD and Agency directives.

Standards:

- Develop, maintain, and execute the COOP-DR Testing and Training Plan. (CDRL A008)
- Maintain disaster recovery and COOP plans, conducting semi-annual failover exercises to provide operational readiness.
- Develop and maintain the Disaster Recovery and Incident Response Plan (CDRL A009) and align with GNOSC SOPs and the government Incident Response Management Plan.
- Conduct annual DR tests, report findings to the PM, and provide compliance updates to the ISSM.
- Monitor security logs, respond to incidents within one hour, resolve them within 24 hours, and escalate as needed.

- Document and report incidents with detailed analysis, provide After Action Reports (AARs) to the COTR within 24 hours, and conduct root cause analysis for recurring issues.
- Mitigate bottlenecks, apply patches per DoD timelines, and maintain DISA STIG-compliant configurations, notify ISSM of security-relevant status updates.
- Coordinate network restoral actions with external providers and OGAs (e.g. DISA, DREN). Assist Mission Partners with communication restoration activities.
- Propose solutions to prevent future issues, implement corrective actions, and reduce incident impacts.
- Maintain detailed records (within 99 % accuracy) of configurations, updates, and incidents while delivering Monthly Status Reports and Quarterly Compliance Audit Reports via automated dashboards.

8.6 Restoration of Enterprise IT services

(Cost Plus Fixed Fee)

The contractor shall provide comprehensive incident management services, including detection, logging, analysis, resolution, and reporting, ensuring rapid restoration of IT services and minimizing disruptions to operations. All activities shall align with Agency and DoD policies, emphasizing continuous improvement and effective communication.

Standards:

- Develop and execute an Incident Management Plan to restore IT services, using monitoring tools, data analysis, and user feedback to identify and log incidents systematically.
- Categorize incidents by impact and urgency, prioritize resolution efforts, and communicate progress and plans via a dashboard.
- Maintain a Monthly Problem Report detailing open problems, resolution times, service impacts, workarounds, and improvement actions and deliver metrics via dashboard.
- Implement workarounds to mitigate immediate impacts while addressing root causes to prevent recurrence.
- Conduct root cause analyses (RCA) and iterative process improvements to enhance system reliability, response times, and customer satisfaction.
- Use automated tools and dashboards to monitor trends, track metrics, and provide real-time updates on incident statuses and resolutions.
- Collaborate with government and internal teams to align with policies and provide transparency in incident management efforts.

8.6.1 Routine Back-Up, Roll-back, Recovery and Restoration Services

The contractor shall perform and maintain routine backups, provide recovery or restoration services. for IC managed or serviced; systems, networks, user accounts, applications, databases, desktop data, to maintain availability, integrity and compliance with DoD and Disaster

Recovery. Continuity of Operations, Incident Response Management, and Cybersecurity Plans and Policies.

8.6.1.1 User Account and Backup and Recovery

The contractor shall perform routine back-ups and recovery of IC managed desktop data to restore user data in the event of system failure.

Standards:

- Periodically test backup, recovery, and rollback processes to support data availability and integrity.
- Maintain records of desktop configurations, service activities, and security compliance checks.
- Document solutions and update a knowledge base to streamline troubleshooting and support.
- Provide real-time reports on support activities, resolution times, and compliance via an automated dashboard.
- Respond to service requests within two hours and resolve issues within 24 hours or escalate as needed.
- Achieve a user satisfaction rating of 95%+ and provide system uptime of 99.9% to support mission-critical operations.
- Deliver monthly service reports to the COTR detailing request types, resolution times, and user satisfaction metrics via an automated dashboard.
- Submit quarterly compliance audit reports to the COTR summarizing findings and remediation actions.
- Provide incident reports within 24 hours, documenting all security incidents and resolution actions.

8.6.1.2 System and Network Backup and Disaster Recovery

The contractor shall establish and maintain network configuration backups and disaster recovery plans to provide quick restoration of services in the event of a network failure.

Standards:

- Implement and test backup and disaster recovery processes to deliver data integrity and availability for critical system, network, application, databases, end-user, and server resources.
- Conduct quarterly backup and recovery tests, documenting results and ensuring RTOs/RPOs meet mission requirements and DoD standards.
- Take corrective actions for recovery failures, retest, and adjust processes as needed to maintain compliance.
- Maintain up-to-date documentation of application configurations, maintenance activities, incidents, and compliance audits, ensuring alignment with Agency and DoD policies.
- Respond to critical incidents IAW DoD 6510.01 within one hour and resolve within 24 hours or escalate as necessary.

8.7 Technology Integration

(Firm Fixed Price)

The contractor shall perform an analysis and findings of potential improvements and technologies that show high promise for returning value.

Standards:

- Present at a minimum three business case analysis for each recommendation that assesses the return against the total investment (both one-time and full life cycle costs) and associated risks (equal to or better capability at a reduced cost) on a yearly basis.
- Address the following in the business case analysis.
    - Demonstrate compliance with federal regulations, program management directives, and the cybersecurity requirements as specified in Task Order 3
    - Demonstrate all recommended security relevant devices are on the Approved Products List (APL)
    - Verify a trusted supply chain for product acquisition and selection
- Display candidate and government accepted improvements within the Management Information System (MIS) dashboard for government review and Government situational awareness

9.0 Portfolio Management Services

(Cost Plus Fixed Fee For RFP Proposal, with eventually transition to FFP over time)

The contractor shall deliver program management services to support mission-critical operations and provide effective oversight of the IT portfolio. The contractor shall enable the government program office to manage, monitor, and make informed decisions regarding enterprise and business management operations while ensuring alignment with organizational goals and regulatory requirements.

9.1 Management Information System (MIS)

The contractor shall establish, maintain, and use a non-proprietary integrated Management Information System (MIS) to support decision-making, coordination, control, analysis, trend visualization, and forecasting within the program portfolio, including requests from Two Letter customers and stakeholders. The MIS shall integrate people, processes, and technology from a portfolio perspective across the entire IT Service Management Life Cycle, encompassing requirement planning, budget authorization, implementation, operation, maintenance, and decommissioning/retirement. The MIS shall be designed to promote agility and flexibility, enabling future capability growth.

Standards:

- Deliver a real-time, continuous, automated reporting capability within six months of award.

- Deliver accurate and timely updates for all project requirements, including cost, schedule, performance, and project milestones.
- Develop and maintain automated dashboards that report:
    - Project Status and Programmatic Information: Key metrics for progress and performance.
    - Service Request Metrics: Including ticket resolution times, first-contact resolution rates, user satisfaction, recurring incidents, and ticket status (open vs. closed).
    - Security and Performance Data: Real-time and historical data on server, network, and application performance, uptime, compliance status, and identified risks/incidents.
    - Network Availability and System Health: Situational awareness with alert notifications for degraded performance and outages.
    - Security Compliance: Findings from monthly access audits and compliance checks, including remedial actions taken.
    - Storage Utilization: Overall storage status and Two Letter element usage of storage assets.
- Provide built-in alert schedules for approaching milestones and notifications when agreed to baseline cost thresholds exceed 85%.
- Provide a capability that can ingest and process multiple report formats and data types, facilitating seamless integration and reporting.
- Create visualization models to depict the health and performance of the program portfolio, highlighting key trends and metrics.
- Archive and retain all data for a minimum of seven years from the time of entry to support future analysis and compliance.
- Track all project phases within the MIS for Two Letter customers.
- Provide multi-level reporting tailored to individual end-users, locations, or funding organizations, as requested.
- Track and report training completion rates, including the percentage of users who have completed required Cyber Workforce training programs.
- Submit a list of software licenses and hardware to be procured for Government approval 180 days before renewal dates and before purchases are made via the MIS. Obtain approval from the COTR for all acquisitions.
- Provide itemized lists of hardware/software, quantities, costs (original and current), running totals, End-of-Life (EoL) and End-of-Service (EoS) dates, Two Letter funding allocations, and user assignments via the MIS dashboards.
- Maintain technical, physical, and administrative control over all authorized software, including a comprehensive inventory in hard and/or digital formats and make inventory results available within the MIS.

9.2 Portfolio Management Plan and Strategy

The contractor shall develop, maintain and execute a Service Portfolio Management Strategy.

Standards:

- Specify the long-range goals of the Service Portfolio Management process, establish roles and responsibilities, and identify any guidelines and/or constraints on the design.
- Analyze all existing infrastructure as part of the requirements engagement process to provide efficient utilization.
- Define the verification methodologies and criteria for each requirement and then tie each one to a specific verification procedure.
- Provide and maintain a Service Portfolio Management Strategy Plan. (CDRL A010).

9.3 Cost Management

The contractor shall provide cost management information for individual customer billing and accounts receivable, defining cost.

Standards:

- Track all Two and Three Letter costs including user usage, consumption and attributes for all IT systems, services and applications within 6 months of contract inception.
- Communicate cost and performance to the stakeholders, alert if schedule and cost exceeds established thresholds.
- Identify project-specific cost controls and manage costs within authorized budget.

9.4 Foreign Military Sales IT Services and Case Requirements

(Firm Fixed Price)

The contractor shall provide capabilities and services to Foreign Military Sales (FMS) office personnel supporting security assistance and FMS activities as outlined in the FMS SLA. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

Standards:

- Provide unclassified and classified end user equipment, software, and printers
- Provide shipping and travel for service personnel
- Provide IT requirements as defined in each Letter of Agreement (LoAs)

10.0 Information Technology Services

(Firm Fixed Price)

10.1 ITSC Objectives and Standards

(Firm Fixed Price)

The contractor shall manage IT service catalog (ITSC) throughout the lifecycle of the service.

Standards:

- Develop, implement, maintain and utilize workflows to allow customers to submit standard service requests that are assigned based on the service request type and customer responses
- Validate the IT Service Request Fulfillment process adheres to government program office IC Portfolio Management Business Rules.
- Follow the Governments Commodity IT Process (IAW current IT Business Rules) to provide request details and cost to the Government for approval prior to procurement.
- Update all service/cost models in the IT service catalog every 6 months.
- Submit for approval "3" new service catalog items every 6 months and report on the status of this analysis in the monthly status report.
- Validate 100% of services have a cost model, and track the cost for Two Letter customer billing.
- Provide customer facing interface to allow customers to view current cost and projected reoccurring cost by Two Letter.
- Document each requirement in the Service Pipeline and Service Catalog to include the requirement's function, stakeholder, resource utilization, including an assessment of existing infrastructure, and prioritization.
- Update the Service Portfolio as requests for new, change, or retirement of services are received from customers and stakeholders within seven calendars days of the required change.

10.2 Solutions Development and Implementation

(Cost Plus Fixed Fee)

The contractor shall develop, implement and deliver IT solutions that meet DoD and Agency compliance requirements throughout the system development lifecycle. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

Standards:

- Track progress and performance against cost and schedule baselines - provide near real time report that includes dependencies and resources to Government Contracting Officer's Technical Representative COTR throughout the lifecycle
- Communicate in writing any cost estimate, schedule, or requirements/scope changes in projects
- Conduct a final project review at project closeout to validate service delivery, transition to Operations & Sustainment (O&S), all artifacts delivered, cost accounts have been closed within 14 days of transition to O&S
- Provide quality assurance and quality control functions consistent with AGILE, Waterfall, ITIL, and PMI standards and best practices by personnel with requisite qualifications
- Develop and automate portfolio briefings for Two Letter reviews as directed by the customer (~4 annually)

- Validate the secure design, development, test, implementation, maintenance, and evaluation of information system security throughout the systems development lifecycle IAW 10.5 Lifecycle Management Standards for IT Assets, 10.7.2 Enterprise Architecture, 10.7.3 IT Systems Engineering and TO XXX 8.3.4 Cybersecurity Project Integration
- Provide end-to-end project management throughout the development lifecycle.
    - Capture Dependencies and resources down to the position number
- Establish and manage dashboard, with monthly reports on project progress, resource utilization, dependencies, compliance status, and risk mitigation activities.

10.3 Customer Relations

(Firm Fixed Price)

The contractor shall provide a customer-focused management plan and strategy for IT service delivery. The contractor shall prioritize effective customer relations, ensuring positive user experiences, efficient communication, and continuous improvement of IT services.

Standards:

- Develop and deliver a Customer Relations Management (CRM) plan. (CDRL A011)
- Streamline and centralize customer interactions, recording responses to enhance service delivery.
- Solicit and analyze customer feedback to identify trends, pain points, and opportunities for improvement.
- Conduct outreach surveys and provide actionable insights to the COTR.
- Utilize automated solutions to handle at least 40% of user inquiries and maintain a self-service knowledge repository with performance dashboards, provide this metric via the MIS dashboard at least monthly.
- Update a quarterly User Experience Tracker with survey data, feedback, recurring issues, and modernization opportunities.
- Minimize day-to-day operational disruptions through detailed planning with customer for upgrades; maximize use of scheduled after business hour maintenance windows for customer impacting work.

10.4 Continuous Improvement (CI)

(Cost Plus Fixed Fee)

The contractor shall establish a CI program to monitor performance, gather feedback, and identify and implement opportunities for cost control, process optimization, and performance enhancements. The program shall align with DoD operational goals and foster a culture of continuous improvement within the workforce. (Note: this task will be moved to paragraph 8.2 for the final RFP)

Standards:

- Monitor IT performance and provide quarterly recommendations to improve response times and user satisfaction.
- Regularly collect and analyze user feedback to identify training, staffing, or resource needs and prioritize CI opportunities.
- Report performance metrics, incident trends, resolution times, and user satisfaction via an automated dashboard.
- Identify at least two cost control, process optimization, or performance improvement opportunities every six months and present them in the Status Report.
- Develop and submit a CI implementation plan, including an Organizational Impact Assessment (OIA) detailing resources, costs, operational impacts, schedules, risks, and training requirements.
- Execute the CI plan, measure outcomes, and report results, including cost savings, in the Task Status Report.
- Recommend process amendments to align government and contractor workflows for improved efficiency, provide these recommendations to portfolio manager at least monthly.

10.5 Lifecycle Management Standards for IT Assets

(Firm Fixed Price)

The contractor shall adhere to lifecycle management standards to maintain accountability and visibility of assets from acquisition through disposition (Throughout the entire Lifecycle). Assets are to be procured, deployed, managed, secured, and retired in compliance with DoD and Agency policies, minimizing risks to operations and maintaining mission readiness.

Standards:

- Identify and assess asset requirements based on mission needs, security standards, and budget constraints, aligning with DoD policies and conducting cost-benefit analyses.
- Develop and deliver Lifecycle Plan within 1 year of contract award (CDRL A007).
- Develop procurement plans, ensuring compliance with DoD acquisition regulations and COTR approvals before purchases.
- Use approved procurement channels, DoD Wide Contracts, maintain third-party support agreements, and validate timely invoice payments.
- Enforce supply chain security by verifying vendor compliance with DoD frameworks like CMMC, TAA compliancy and documenting asset specifications, warranties, and contracts.
- Deploy assets securely, adhering to DISA STIGs and DoD security standards, configuring EDR tools, integrating with ICAM systems, and recording details in the CMDB.
- Maintain assets through regular security assessments, patch management, performance monitoring, and preventive maintenance, ensuring SLA compliance.
- Decommission assets securely, following data sanitization standards, updating the CMDB, and disposing of assets through authorized channels.
- Conduct lifecycle management audits, ensuring RMF and cybersecurity policy compliance, and monitor assets for vulnerabilities and incidents.

- Track asset usage, service association, and lifecycle phases, providing metrics on inventory usage, security compliance, cost reductions, and secure disposal.
- Review and update lifecycle policies regularly, incorporating stakeholder feedback, emerging technologies, and evolving mission needs.
- Enforce supply chain risk management best practices to enhance cyber resiliency and conduct annual audits to validate alignment with DoD and agency policies.

10.6 Configuration and Change Management (CM/ChM)

(Firm Fixed Price)

The contractor shall implement and maintain a unified Configuration Management (CM) and Change Management (ChM) program to systematically manage IT system configurations and changes in an effective manner to minimize disruption to the mission. The integrated program shall provide system integrity, minimize disruption, maintain security, and align with ITIL best practices, NIST SP 800-128, and DoD RMF standards.

Standard:

- Develop and deliver a Configuration and Change Management Plan (CCMP) outlining processes, risk management, and validation protocols (CDRL 012).
- Assess, prioritize, and present significant Change Requests (CRs) to the CAB for approval, executing and validating approved changes, and documenting lessons learned.
- Conduct security impact assessments, detect unauthorized changes, and update configuration baselines post-change.
- Identify, baseline, and document all Configuration Items (CIs), including hardware, software, and networks, ensuring alignment with operational and security standards.
- Standardize change management processes to prevent unauthorized changes and validate all changes are reviewed, tested, implemented, and validated against baselines.
- Maintain an authoritative CMDB to track CIs, relationships, and updates, ensuring >98% accuracy and reflecting the as-built state post-change.
- Conduct annual Configuration Audits and provide metrics on Change Success Rate (>90%), CMDB Accuracy (>98%), and post-change incident rates (<5%).
- Develop a Forward Schedule of Change (FSoC) to plan and communicate authorized changes.
- Notify stakeholders monthly about changes, impacts, and risks, and provide updates on change outcomes and metrics.
- Provide initial and annual refresher training on CM/ChM processes and tools, ensuring knowledge transfer for operational continuity.

10.7 Engineering Architecture Management

(Cost Plus Fixed Fee)

10.7.1 IT Reform, Strategy, and Transition Planning

The contractor shall develop and implement strategies that improve user experience and increase mission success while maintaining compliance, cybersecurity, speed of delivery and improving performance and efficiency.

Standards:

- Develop and deliver 3-year and 5-year IT strategies with updates annually that align with Federal, DoD and agency policy and compliance requirements. Reference Information Technology Updates and Refreshment Strategy Plan (CDRL A013).
- Identify opportunities to automate recurring labor-intensive activities to maximize available resources, gain efficiencies or process improvements. Maintain an authoritative source of improvement topics which the government can review on demand and select candidate items that can be implemented upon availability of resources. Include expected level of resources to implement, timeline, the future reduction in resources, and return on investment.

- Develop, maintain and improve automated system including input from user experience satisfaction surveys and profiling tools that track and identify user experience issues. (e.g. unresponsiveness, crashing, packet drops, inefficient data flows, time to load an application)Establish a system profile baseline (performance characteristics) and capture changes, improvements, or degradation in user experience on a quarterly basis.

10.7.2 IT Enterprise Architecture

The contractor shall develop and use IT architectures that maximize value, improve user experience, maintain compliance, includes cybersecurity requirements, articulate interdependencies and interfaces, and enable governance and oversight. The contractor shall achieve interoperability by including various disciplines for architecture development and review such as cyber, implementation, operations and sustainment, and customer stakeholders.

Standards:

- Create and maintain an authoritative architecture repository using MBSE tools compliant with Federal and DoD standards, accessible to stakeholders without additional software, and integrated with eMASS for DoDAF views.
- Update and review DoDAF views semi-annually, delivering to the System ISSM, and provide efficient linkage and propagation of changes across related artifacts.
- Maintain version control for all approved architecture artifacts and recommend DoDAF views for government approval during project requirements phases.
- Align architectures and artifacts with traceable business and technical requirements, IT Strategic Plans, and Federal/DoD initiatives, incorporating capacity limits and identifying bottlenecks.
- Develop reusable reference architectures using capacity-based parameters and perform semi-annual reviews to maintain alignment with approved baselines.
- Notify the government of changes to as-is architectures for approval, transitioning to to-be architectures with minimal rework.
- Identify, track, and address architectural risks and provide automated portfolio briefings for Two Letter reviews.

10.7.3 IT Systems Engineering

The contractor shall engineer IT solutions that improve user experience, yield best value against requirements, includes comprehensive cybersecurity engineering and review, and enables governance and oversight.

Standards:

- Utilize the authoritative IT architecture and engineering repository for all managed IT that contains contractor developed and maintained automated build, configuration and test files in support of IT orchestration. The ability to review must be accessible via web browser to promote broad access.
- Create and execute a common standard operating procedure to maintain version control of all engineering files within the repository.
- Create and validate system technical, performance, functional, and compliance requirements that are testable and link to customer and business objectives.
- Develop automated technical evaluation and regression tests as part of the new capability delivery.
- Iteratively validate the capability against customer requirements using stakeholder participation during solution development and implementation.
- Leverage an automated and repeatable implementation and configuration mechanism to create and maintain the customer desired capability.
- Conduct quarterly comprehensive assessment using existing automated tests against the deployed solution and post the findings in the engineering repository.
- Determine if each finding from quarterly assessment results in a test modification or reverting the change back to baseline architecture and engineering repositories.
- Provide an assessment of risks and impacts, including interdependencies, an implementation plan, evaluation criteria for successful implementation and a rollback plan in the event of failure.

11.0 Collateral Support Services

(Firm Fixed Price)

The contractor shall provide services including service desk operations, technical support, incident resolution, account management, hardware and software troubleshooting, user training, and ensuring compliance with security and operational standards. Services shall be delivered in accordance with the agency's Tiered Support Definition document and applicable Agency and DoD policies.

11.1 Integrated Service Desk (Tier I & II)

(Firm Fixed Price)

The contractor shall provide comprehensive IT Service for end-users. Responsibilities include installing, configuring, maintaining, and troubleshooting IT systems, peripherals, and software. The contractor shall validate that user environments comply with Agency and DoD security standards and are maintained in alignment with DoD operational requirements.

Standards:

- Respond to service calls within 90 seconds and resolve 95% of incidents on first contact using an approved ticketing system.
- Install, configure, and maintain desktop/laptop systems, version control and peripherals, ensuring operational readiness and security compliance.
- Deploy and manage software, operating systems, and security updates, utilizing automated solutions to deliver packages within 48 hours of receipt and authorization.
- Perform regular maintenance, updates, and security patching in alignment with DoD and agency standards.
- Manage enterprise print services, including monitoring consumables and supporting user equipment moves (~50 per week).
- Handle user account management, access controls, and password resets, adhering to zero trust architecture and DoD security protocols.
- Provide IT training and maintain a self-service knowledge base (Tier 0) for common issues and resolutions.
- Maintain cybersecurity awareness and keep agency workforce apprised of cybersecurity threats and policy updates weekly.
- Provide a capability to submit surveys after every incident and service request and give the customer an opportunity to submit surveys after their interactions.
- Establish and maintain a formal complaint and escalation process

11.1.1 IT Services for Premium Users

The contractor shall provide IT services to approximately 70 premium users designated by the government. Services include advanced technical support, data migration, issue resolution, and break/fix services for a variety of devices and systems. The contractor shall adhere to strict performance and response standards while ensuring compliance with agency and DoD policies.

Standards:

- Deliver technical assistance and support for hardware, software, network, and access issues.
- Manage ticketing systems, fulfill user requests, and provide telephonic troubleshooting and issue resolution.
- Apply registry fixes, develop scripts to address user-specific issues, and resolve complex system errors.
- Perform data migrations between computers/systems with minimal downtime and errors.
- Provide repair and support for desktops, laptops, printers, mobile devices, tablets, thin clients, thick clients, and peripherals.
- Install and verify security patches, software updates, and firmware upgrades in accordance with agency and DoD policies.
- Provide 24x365 on-call IT services to provide uninterrupted support for Premium Users.
- Respond to Premium User notifications within one (1) hour of receipt.

- Achieve a 99% first-call resolution rate for all reported issues.

11.2 Tier III Services

(Firm Fixed Price)

The contractor shall deliver Tier 3 support for backend IT services, including advanced troubleshooting, root cause analysis, system optimization, and proactive maintenance. The services encompass both classified and unclassified environments and address all aspects of backend infrastructure, including servers, databases, storage systems, and enterprise applications.

Standards:

- Handle escalated incidents from Tier 1 and Tier 2, performing root cause analysis (RCA) and implementing permanent fixes to prevent recurrence.
- Document resolutions and lessons learned for Tier 1/2 knowledge bases, optimizing backend systems for performance, scalability, and reliability.
- Implement configuration changes and updates in alignment with DoD and agency policies, performing proactive maintenance to prevent operational disruptions.
- Monitor backend infrastructure with approved tools, providing alerts for performance, security, or reliability issues.
- Enforce compliance with DoD RMF and cybersecurity policies, including implementing security measures, conducting audits, and maintaining eMASS artifacts.
- Collaborate with development, operations, and security teams to resolve complex issues and escalate critical problems to specialized teams or vendors as needed.
- Maintain accurate records of system configurations, maintenance, and incident resolutions.

11.2.1 Server Administration

The contractor shall perform server installation, configuration, monitoring, maintenance, and security for both physical and virtual environments. This includes applying security controls, enforcing compliance, and delivering proactive system management to protect the operational efficiency and security of the server infrastructure.

Standards:

- Deploy and configure enterprise servers in physical and virtual environments to meet operational and mission requirements, adhering to DoD and Agency standards.
- Create and maintain hardened master OS configurations, ensuring compliance with cybersecurity requirements and secure network integration.
- Tailor backup and recovery processes to prioritize High, Medium, and Low assurance systems for rapid restoration.
- Perform server maintenance, including troubleshooting, performance optimization, and preventive tasks like firmware upgrades and hardware replacements.

- Monitor server availability and performance to provide uninterrupted operations, applying security measures such as firewalls, access controls, encryption, and audit logging.
- Review and apply security updates IAW RMF and Cyber Tasking Orders, conduct vulnerability assessments, and implement patches to maintain system integrity and mitigate risks.

11.2.2 Network Administration

The contractor shall provide comprehensive network administration services for networks, including the operation, configuration, monitoring, and maintenance of network systems at approximately 190 global sites and 500 enclaves. The contractor shall ensure network availability, performance, and security meet DoD standards. The contractor shall safeguard availability, performance, and security of both classified and unclassified network environments.

Standards:

- Configure and manage network devices (routers, firewalls, VPNs, SDNs, IDS/IPS, proxies, load balancers, etc.), ensuring alignment with DoD standards.
- Implement firewall changes upon approval, maintaining detailed configuration records and topology diagrams.
- Deploy and manage network monitoring tools to track traffic, device health, and performance, addressing issues promptly to minimize disruptions.
- Perform updates, patching, and access control audits to validate compliance with DoD security policies and least-privilege requirements.
- Configure multifactor authentication and enforce security measures like encryption and intrusion prevention for privileged accounts.
- Monitor network availability using approved tools, providing automated alerts and dashboards for stakeholders.
- Conduct root cause analyses for disruptions, implement corrective actions, and maintain compliance artifacts in eMASS.
- Notify government of network changes and maintain updated documentation for configurations, maintenance, and incidents.

11.2.3 Telecommunication Administration

The contractor shall provide comprehensive telecommunications administration services for the operation, maintenance, and management of communication infrastructure supporting DoD requirements. Services include oversight of telecommunication hardware and software for classified and unclassified environments.

Standards:

- Operate and maintain network communication infrastructure, including mobile device managers, ensuring adherence to Agency Wiring Configurations and standards.
- Verify and document telecommunication service orders within 24 hours of completion and implement provider-issued actions.
- Maintain and troubleshoot telecommunication hardware, software, and backbone layers, resolving issues and reporting incidents within one hour of detection.
- Monitor and optimize network performance, addressing latency, reliability, and vulnerabilities (e.g., SPoFs), and provide automated alerts to stakeholders.
- Coordinate alternate routing during outages (critical: 1 hour; non-critical: 48 hours) and restoration activities with providers and OGAs.
- Comply with DoD standards, applying encryption and securing backups, while notifying government representatives of system changes.
- Deliver monthly performance reports and after-action summaries to the COTR via the MIS dashboard, addressing circuit utilization, trends, and reliability metrics.
- Provide 24/7/365 incident response, resolve issues promptly, and document outcomes per GNOSC SOPs.
- Develop contingency plans, maximize maintenance windows, and maintain effective communication methods and contact information.

11.2.4 Guest Network Services

The contractor shall operate, maintain and manage guest network services (both wired and wireless). The contractor shall ensure secure, reliable, and high-performance connectivity for users and devices across all supported sites.

Standards:

- Operate and maintain wired and wireless guest networks, ensuring uninterrupted service and adherence to security best practices.
- Configure and manage network infrastructure, including switches, access points, routers, and wireless controllers.
- Monitor and troubleshoot network traffic, performance, and security issues, resolving them promptly.
- Manage user access and implement secure guest authentication through captive portals.
- Optimize wireless coverage and performance via site surveys, signal analysis, and strategic access point deployment.
- Perform regular updates, patches, and compatibility checks to support a wide range of guest devices.
- Maintain communication methods and accurate contact information for effective outage notifications and coordination.

11.2.5 Point of Sale (POS) support

The contractor shall operate, maintain, and manage of Point of Sale (POS) systems across all supported sites. This includes ensuring secure, reliable, and high-performance connectivity for POS devices, as well as implementing measures to safeguard sensitive transaction data. Services shall align with DoD standards and industry best practices to maintain compliance, security, and operational efficiency.

Standards:

- Operate, maintain, and manage POS network infrastructure to ensure seamless transactions and minimal downtime.
- Monitor, resolve connectivity issues, and implement security measures like encryption to protect sensitive data, adhering to PCI DSS and DoD standards.
- Collaborate with vendors for updates and compliance while conducting audits and root cause analysis to prevent recurring issues.
- Detect, log, and report incidents within one hour, notifying government representatives of security concerns.
- Provide monthly performance reports with metrics (uptime, latency, transaction success rates) and maintain comprehensive documentation of configurations, maintenance, and updates.
- Minimize disruptions through scheduled maintenance and deliver after-action reports for major incidents and activities.

11.2.6 Storage Administration

The contractor shall manage all facets of storage administration, including installation, configuration, maintenance, monitoring, optimization, and security. Services shall encompass storage lifecycle management and compliance with applicable DoD policies and regulations to meet operational requirements and mission objectives.

Standards:

- Design, configure, and manage enterprise storage systems (SAN, NAS, cloud-based) to meet scalable and secure mission requirements.
- Integrate with DoD network systems, monitoring storage performance, capacity, and health with approved tools.
- Conduct preventive maintenance, address performance bottlenecks, and resolve hardware or connectivity issues.
- Implement comprehensive backup and recovery strategies, validate backups, and test recovery processes semi-annually.
- Apply security controls, including encryption, access management, and audit logging, while performing regular vulnerability assessments and patching.

- Maintain detailed storage documentation, including configurations, maintenance logs, and incidents.
- Provide a weekly report to the COTR on storage utilization, backup and recovery status, and compliance with DoD policies via a dashboard.
- Resolve service interruptions, validate data availability, provide application support, perform capacity planning, and deploy storage configurations.

11.3 Application Administration

(Firm Fixed Price)

The contractor shall provide comprehensive application administration services, including installation, configuration, maintenance, monitoring, troubleshooting, and security of web services, databases, and other enterprise applications. Services shall support both classified and unclassified environments, providing seamless operations and compliance with DoD and Agency standards.

11.3.1 General Application and Web Administration

The contractor shall perform design, deployment, configuration, and maintenance of applications and web services while ensuring their security, availability, and compliance with Agency and DoD cybersecurity policies. Services include monitoring, performance optimization, and collaboration with internal teams and external vendors as required. Applications include Commercial off the shelf (COTS), government off the shelf (GOTS), and all other services delivered by a web or application server.

Standards:

- Design, deploy, configure, monitor, harden, patch, and document application and web administration, ensuring availability, security, and performance in compliance with DoD standards.
- Apply security controls, including encryption, access management, and audit logging, while conducting vulnerability assessments and implementing patches.
- Collaborate with vendors and administrators for SME support and proper application integration into operational environments.
- Monitor and optimize application performance using approved tools, addressing bottlenecks and ensuring seamless functionality with minimal disruptions.
- Manage user roles, permissions, and access controls, adhering to least privilege and zero trust principles.
- Maintain detailed documentation of configurations, SOPs, maintenance, and incidents, reviewing and updating annually or as changes occur.
- Provide a weekly report on performance metrics, security compliance, change management, and resolved incidents with corrective actions.

11.3.2 General Database Management and Administration Services

The contractor shall provide comprehensive support for database management and administration. Services include installation, configuration, performance tuning, maintenance, troubleshooting, and security of database systems. These services support both classified and unclassified environments, ensuring data integrity, availability, and scalability. Databases include but are not limited to Oracle, Microsoft SQL Server, Cassandra, Postgres SQL, Mongo DB and MySQL.

Standards:

- Design, deploy, and optimize secure database solutions to meet mission and operational needs, collaborating with stakeholders to identify requirements and implement best practices.
- Document database architecture, including schemas and relationships, and maintain comprehensive documentation of configurations, SOPs, maintenance, and incidents, updated annually or as changes occur.
- Install, configure, and maintain high-availability database systems, applying performance tuning and security hardening measures.
- Monitor database performance, resolve bottlenecks, and address query inefficiencies using approved tools.
- Conduct routine maintenance, including backups, indexing, and storage optimization, while implementing and testing comprehensive backup and recovery strategies.
- Manage user roles and access controls based on least privilege and zero trust principles and collaborate with cybersecurity teams to address incidents and comply with DoD policies.
- Perform vulnerability assessments, apply patches, and implement security controls such as encryption, access management, and audit logging.
- Provide regular reports on performance, backup and recovery readiness, security compliance, and resolved incidents with corrective actions.

12.0 Infrastructure Services

(Firm Fixed Price)

The contractor shall manage the full lifecycle of cable infrastructure, including replacement, testing, repair, installation, termination, and removal of cabling. Services shall encompass both classified and unclassified environments and include the operation and maintenance of network connections, adherence to industry standards, and active support for Agency operations.

Standards:

- Comply with the Information Technology Infrastructure Installation Guide, IC 8350.01
- Replace, repair, test, and maintain secure and non-secure voice, video, and data cable infrastructure at principal locations, adhering to TEMPEST, NECA, and BICSI 568 standards.

- Execute cable plant management activities and maintain a government-approved tracking system, documenting connections to external networks.
- Perform cable-plant management services which include copper, fiber optic, RF, and specialized cabling, installing, terminating, and testing new cabling and removing obsolete lines.
- Mark and label cabling per industry and Agency standards, obtain a 99.9% reliability rate, excluding scheduled maintenance.
- Operate and maintain network connections between the Agency, external Government, and contractor facilities, supporting planning, execution, and after-action phases of operations.
- Complete all maintenance and testing within SLA timelines.

13. 0 COMSEC Services

(Firm Fixed Price)

The contractor shall act as the Communications Security (COMSEC) "alternate" COMSEC Manager system-controlling authority.

Standards:

- Manage, store, and issue encryption equipment and keys, tracking effective dates to provide timely replacements, and assist the Government COMSEC Manager with cryptographic lifecycle management (LCM).
- Control, ship, receive, and manage Controlled Cryptographic Items (CCIs) and act as Controlling/Command Authority for government-controlled keys.
- Administer COMSEC briefings and debriefings for cleared personnel with a valid NTK, maintaining documentation for all COMSEC actions.
- Provide 100% COMSEC inventory accountability, including ordering, issuing, auditing, and destroying key material, and update COMSEC publications within 60 days of required changes.
- Manage and validate CCIs, perform maintenance, and support Over-the-Air Re-keying and Distribution (OTAR&D).
- Serve as a liaison between the COMSEC Account Manager, site managers, engineers, and users, following the COMSEC Plan and SOPs.
- Expedite equipment repairs and coordinate testing of cryptographic items, ensuring compliance with NSA and Homeland Defense requirements.
- Track and manage key and equipment lifecycle, addressing End-of-Life (EOL) per NSA Crypto-Modernization, and submit equipment for destruction.
- Administer and maintain USTRANSCOM Form 10, manage Defense Courier Division (DCD) shipments, and comply with shipping protocols.
- Configure, issue, and maintain secure voice devices (e.g., STE, vIPers), supporting firmware updates and training users on operation and re-key procedures.

- Maintain secure voice inventory, conduct semi-annual re-key verifications, and store inactive briefings for 5 years.

14.0 Sensitive Compartmented Information Facility/Special Access Program (SCIF/SAP) Support Services

(Firm Fixed Price)

The contractor shall provide comprehensive SCIF/SAP end user services, including service desk operations, technical support, incident resolution, account management, hardware and software troubleshooting, and user training. Services shall encompass support for SCIF/SAP environments across the enterprise, addressing both classified and unclassified systems.

Standards:

- Provide IT services for SAP, OGA, and JWICS systems, including mission-specific and TS/SCI-level systems, with active support at principal and remote locations.
- Perform ISSE and ISSO functions for TS/SCI systems, ensuring cybersecurity compliance, operational sustainment, and lifecycle management.
- Maintain relationships with DIA JWICS providers to support high service availability and implement a Continuous Service Improvement (CSI) program with monthly reports.
- Execute Problem Management and Risk, Issue, and Opportunity (RIO) Management processes, providing Tier I/II Service Desk support for SCIF/SAP users with 18/5 availability and 24/7 mission-critical support when authorized by the government.
- Utilize an approved ticketing system to resolve 95% of incidents on first contact, communicate updates to users, and provide timely ticket resolution.
- Configure and maintain IT peripherals, promote self-service through an updated knowledge base, and enforce RMF compliance for access control and user privileges.
- Maintain real-time IT asset inventory via an automated dashboard, conduct root cause analyses for recurring issues, and implement long-term solutions.
- Deploy and configure SCIF/SAP IT hardware and software, applying updates and patches to meet security and operational standards while maintaining licensing compliance.

15.0 Data Center Management & Operations

(Firm Fixed Price)

The contractor shall perform comprehensive data center management services, encompassing storage, compute, and facility management, including Intermediate Distribution Frame (IDF) and Main Distribution Frame (MDF) areas. Services include proactive monitoring, operational support, disaster recovery (DR), configuration management, and compliance with DoD standards.

Standards:

- Achieve and sustain 99.9% availability of data center services through coordination with operational elements and adherence to GNOSC procedures.
- Provide 24/7/365 support, manage physical environments, and execute authorized changes following Release Control Management policies.
- Troubleshoot and resolve IT service interruptions, documenting root causes and corrective actions, and adherence to SLAs.
- Manage rack space, assignments, and track assets with accurate labeling and quarterly validation of rack elevations.
- Maintain hardware, software, and facilities for failover/recovery, supporting DR requirements in physical and virtual environments.
- Oversee data center facilities, including electrical and environmental IT needs, while adhering to Configuration Management processes.

16.0 Cloud Services

(Firm Fixed Price)

The contractor shall maintain and manage off-premises cloud services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The contractor shall provide secure, scalable, and cost-effective cloud solutions to support mission-critical activities, including migration, provisioning, and management of applications, systems, and data within the cloud environment. Services include cloud governance, application and system migration, infrastructure automation, and compliance with DoD and Agency standards.

Standards:

- Contribute to the agency's Cloud Computing CONOPS by focusing on IT modernization through cloud-based architecture and agile governance practices.
- Provide accurate and timely Cloud billing by 2-letter to MDA/ICP with 5 days of receipt of billing.
- Develop automated cloud management solutions to reduce costs and schedules, including provisioning IaaS, PaaS, and SaaS with repeatable configurations.
- Deliver scalable, elastic, and cost-efficient environments to meet mission needs, while enabling customer self-management of cloud resources.
- Assess applications for cloud migration, manage iterative migrations, and leverage automation for workload and migration management.
- Facilitate quarterly planning sessions with stakeholders to establish sprint objectives and form agile teams to address prioritized activities.
- Report progress using six key metrics: work in progress, completion rates, duration, consistency, and delivery timelines.
- Mitigate security vulnerabilities with automated responses, comply with DoD RMF standards, and execute mitigation strategies for security events.
- Enable continuous deployment with performance monitoring and issue detection using advanced tools.

- Develop processes and policies for Virtual Desktop Infrastructure (VDI) services, including a VDI Service Catalog.
- Offer tailored cloud-based managed services aligned with business strategies and allocate skilled staffing with progress reporting in defined increments.

17.0 Development Security Operations (DevSecOps)

(Firm Fixed Price)

The contractor shall maintain scalable DevSecOps services to enable the rapid delivery of the software development lifecycle (SDLC) and system operations. The contractor will implement Agile methodologies, automation, and continuous integration/continuous delivery (CI/CD) pipelines to accelerate software deployment while ensuring compliance with DoD and Agency cybersecurity and operational standards.

Standards:

- Develop and refine, through the use of automation and Infrastructure as Code (IaC), the ability to build and operate multi-tenant shared services
- Develop and maintain required automation and tooling to quickly deploy and manage cloud resources cloud native services and applications.
- Collaborate with stakeholders to integrate mission requirements into workflows.
- Provide training and knowledge transfer to end users.
- Integrate cybersecurity measures into all phases of the SDLC in compliance with Risk Management Framework (RMF) and NIST SP 800-53
- Maintain system scalability, reliability, and uptime through robust monitoring and incident response frameworks
- Provide independent verifications & validation (IV&V) software assurance pipelines (Including test procedures and validation plan, and automation of the pipelines)
- Deploy Integrated Development Environment capabilities enabling software independent verifications & validation (IV&V) activities
- Support the establishment of threat data repository and transfer of threat data.
- Promote collaboration across development, operations, and cybersecurity teams through standardized tools and processes.
- Implement and analyze functional capabilities and tools for current and future Continuous integration (CI) and continuous delivery (CD).
- Comply with Data Protection Requirements, to include data separation and RBAC controls.
- Automate at least 80% of testing and deployment processes within 180 days of contract award.
- Provide 100% alignment with defined DoD security baselines and Secure Software Development Framework (SSDF).
- Deliver complete and accurate documentation for all processes, configurations, and tool integrations within 5 business days of implementation.
- Deliver evidence of compliance with IAW with DoD and Agency cybersecurity standards.
- Deliver Incident Response Logs Records of all resolved incidents with root cause analyses.

- Develop and maintain Operational Dashboards of near Real-time monitoring and performance metrics.
- Optimize solutions for financial and computational efficiency, provide progress reporting improvements from using existing Non-Standard practices to Standard practices to the COTR monthly.
- Provide provisioning, network and boundary configuration, identity and access management and cybersecurity in support of deploying Assess and Authorize and Modeling and Simulation requirements.
- Install, configure and maintain containers and virtual infrastructure for Analysis Capability and high-performance computer resources to execute medium fidelity simulation.

18.0 Model-Based System Engineering (MBSE)
(Firm Fixed Price)

The contractor shall support the development and sustainment of system engineering activities. The tools shall support the integration of system requirements, design, performance, and verification across the program lifecycle.

Standards:

- Maintain MBSE applications in compliance with Agency and DoD cybersecurity standards and policies.
- Maintain the availability, security, and performance of applications critical to Agency missions.
- Provide technical support and troubleshooting to resolve interrupted application access and functionality.
- Continuously update and maintain applications, implementing patches and upgrades as required by Agency and DoD guidelines.
- Install, configure, and deploy applications in accordance with Agency and DoD standards, ensuring secure and efficient operation.
- Manage application settings and configurations to meet specific operational and security requirements.
- Collaborate with system and network administrators to validate applications are properly integrated into the Agency and DoD infrastructure.

19.0 Integrated Digital Data Environment (IDDE)
(Firm Fixed Price)

This supports the agency mission for the management, maintenance, and enhancement of the Department of Defense's Integrated Digital Data Environment (IDDE). The contractor shall provide comprehensive IDDE management services, ensuring a secure, scalable, and user-friendly platform to support the integration, accessibility, and security of digital data to improve collaboration, operational efficiency, and informed decision-making across the enterprise.

Standards:

- Develop data requirements and aggregate disparate data sources into integrated views of the data and develop all data models, views, and source-to-target mappings at the foundation and aggregate levels.
- Develop and deliver repeatable process, model, and/or other documentation for other programs to follow for Agency-wide data integration requirements.
- Deliver seamless integration of diverse datasets and tools into the IDDE.
- Maintain compliance with DoD and Agency cybersecurity and data governance policies.
- Enhance user experience through training, documentation, and support services.
- Maintain Performance Standard Acceptable Quality Levels (AQL)
    - Provide 99.9% uptime for all IDDE components. Downtime does not exceed 4 hours per month.
    - Integrate 100% of approved datasets within timelines.100% accuracy in data integration processes.
    - Achieve compliance with DoD, FedRAMP and Agency standards. No critical or high-priority vulnerabilities.
    - Provide user training within 30 days of onboarding.
        - 90% user satisfaction in post-training surveys.
    - Respond to support tickets within 24 hours.
        - 95% of tickets resolved within 5 business days.
- Participate in in status briefings, working-level meetings, and other information gathering/dissemination forums.
- Provide integration of Digital Engineering applications across technical and programmatic applications and databases supporting Digital Engineering and modernization.

20.0 Federated Identity Management / Automated Access Provisioning
(Firm Fixed Price)

The contractor shall provide Federated Identity which supports standard Federated protocols and legacy systems for authentication and single-sign-on (SSO) that is scalable to enable the sharing of resources across multiple legacy Identity and Service Providers across unclassified and classified environments.

Standards:

- Deliver Authoritative Identity and Access Management security architecture(s) that enables automated access provisioning and user on-boarding that minimizes access to resources, i.e. data, computing resources, and applications, to only those users identified as needing access.
- Provide automated access provisioning and deprovisioning capability able to onboard and offboard users consistent with least privileged access requirements.
- Implement approval workflows and onboard for federated authentication and automated access provisioning
- Migrate ADFS applications to federation server for authentication and single sign-on (unclassified and classified)

- Establish user access to networks, applications and programs across federated organizations using the same digital identity and credentials.
- Implement agile methodologies and lean startup practices to employ continuous delivery and instill a team dynamic that responds well to change.

21.0 Cross Domain Solution Services

(Firm Fixed Price)

The contractor shall configure, operate and maintain Cross-Domain Solutions (CDS) throughout the entire System Lifecycle (SLC).

Standards:

- Provide engineering, development, Test and Evaluation (T&E), implementation, and A&A services for automated access or transfer of information between two or more differing security domains for the timely sharing of authorized information critical.
- Implement the fully integrated six-phase process of the DISN CDS Approval and Connection process. Note: If an existing solution is determined to meet requirements, only Phases 4–6are required.
  - Phase 1—CDS Categorization and Criticality Determination: Perform the security categorization and criticality determination for the system.
  - Phase 2—Select Security Controls: Identify the appropriate security controls;
  - Phase 3—CDS Security Control Implementation: Implement and document the security controls as required by the CDTAB and IAW the deliverables identified in DoDI 8540.01, Enclosure 4.
  - Phase 4—CDS Security Control Assessment: Validate implementation of security controls and remediate any outstanding security findings. Coordinate Security Control Assessor (SCA) activities. Present the assessment results and security control assessment plan to the Cross-Domain Technical Advisory Board (CDTAB) for review and approval.
  - Phase 5—CDS Authorization: Support SCA activities while they perform the site security control assessment in order to provide approval recommendations to the AO.
  - Phase 6—Operational CDS Monitoring: Perform continuous monitoring activities for CDS. Revalidate requirement annually.
- Deliver documentation for knowledge transfer to provide operational continuity for cross domain solutions.
- Present these results to the DSAWG for approval.
  - Mitigate any additional findings regarding risk, perform additional engineering and testing until approved.
- Identify filters to control access to the stored data.
  - Using attributes associated with user-, network-, application-, and device-authorized clearances.

22.0 Dedicated Customer System Support (Customer Funded)

(Firm Fixed Price)

The contractor shall validate that the IT services and resources are administered, acquired, managed, operated, and cyber defended in compliance with the goals and directives of existing

statutes and DoD issuances and the priorities under the MDA Director and customer leadership. The contractor shall execute both the cybersecurity and IT Cyberspace Operations actions required to operate and protect DoD IT systems across classified networks. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

Standards:

- Perform the full range of cyberspace tasks as identified in the DoD Cyber Workforce Framework to obtain and maintain compliance for the customer environments.
- Provide onsite general IT / Cybersecurity support to satisfy all end user immediate needs.
- Provide end-user training on common IT systems, software applications, and cybersecurity best practices, ensuring personnel are capable of utilizing the tools necessary to perform their duties effectively.
- Coordinate break/fix actions with the base for services provided by the host base if services are provided by the host base.
- Provide IT services for installing, maintaining, and monitoring all network equipment on multiple-level classification networks and working with engineers and the IT Services team in at principal sites.
- Follow Configuration Management processes and tasking IAW customer policies.
- Perform regular health checks to validate system integrity, identify vulnerabilities, and enhance operational performance.
- Monitor workload and trending data to validate the level of support is consistent with the demand and performance metrics requested.
- Document and report findings in accordance with Agency guidelines
- Conduct system maintenance, develop and update maintenance SOPs and checklists, and maintain system maintenance records/logs.
- Automate re-occurring tasks using scripting tools/languages.
- Address any issues identified during health checks or system monitoring promptly.
- Perform root cause analysis for recurring issues and implement corrective actions.
- Coordinate efforts to resolve Incident Requests (break/fix), CRQs (RFC), and Problem Management activities.
- Obtain approval from operations/engineer teams and IT or network security teams before performing security related activities.
- Apply all security patches, firmware updates, and operating system updates promptly upon release and in accordance with established DoD and Agency approved timelines.
- Verify patch installations through system scans and compliance tools (e.g., ACAS, Tanium).
- Document, report, and escalate non-compliance to ISSM team and PM for resolution.
- Provide systems engineering/architect work associated with technical requirements, such as networking, system evaluation, system security, and general

knowledge of data flow within the network, and utilize approved toolsets to document network configurations as required.

- Perform security administration tasks IAW the standards outlined in 8.8 Security Administration
- Perform an analysis of findings to identify potential improvements and IAW 8.9 Technology Integration
- Adhere 10.3 Lifecycle Management Standard Plan
- Conduct Logistics and Product Support management to IAW XXX
- Develop, integrate, operate, and maintain network services IAW 10.6.1 Network Operations and Sustainment (O&S)
- Monitor networks for performance and degradation of service impacts IAW 10.6.3 Network Performance Monitoring
- Maintain cable infrastructure labeling standards IAW 10.6.7 Infrastructure Services
- Manage all asset IAW In accordance with XXX Cyber Tracking and Reporting
- Validate vulnerability management activities are compliant IAW 10.2.5 Cyber Tracking and Reporting
- Perform self-assessments of systems and networks IAW 8.3.1.1 Local Control Center (LCC)
- Assess systems and networks to validate the environment(s) are in a "ready state" IAW 8.3.1.2 Local Control Center (LCC)
- Perform Tier III monitoring and reporting IAW 8.3.1.3 Local Control Center (LCC)
- Continuously monitor managed networks IAW 8.3.2.1 Cybersecurity Configuration
- Manage Ports, Protocols and Services Management (PPSM) 8.3.2.2 Cybersecurity Configuration
- Perform security assessments on Information Assurance enabled hardware IAW 8.3.2.3 Cybersecurity Configuration
- Perform code analysis and provide software risk assessment. (~50 new submissions annually) IAW 8.3.2.4 Cybersecurity Configuration
- Implement TEMPEST countermeasures for areas approved to process, store or discuss classified IAW 8.3.2.5 Cybersecurity Configuration
- Conduct cybersecurity support IAW 10.3.3.1 Risk Management Framework (RMF)
- Verify and validate system security is throughout the development lifecycle IAW 8.3.3.2 Risk Management Framework (RMF)
- Provide COMSEC support IAW 13.0 Comsec Services.
- Provide representation for customer IT-related meetings and act as liaison between customer and Office of the CIO.

22.1 DV

The contractor shall configure, operate and maintain the DV High Performance, High Compute, Classified Enterprise Lab infrastructures located at PMRF, KAFB, VSFB, FGA IAW DoD and Agency requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 22.0 Dedicated Customer System Support

22.2 DX Facility Related Control System (FRCS)

The contractor shall perform device, equipment, and system-level cybersecurity configuration and day-to-day security operations of control systems, including security monitoring and maintenance along with stakeholder coordination to validate the system and its interconnections are secure in support of mission operations located at XXX.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 11.0 Dedicated Customer System Support

22.3 SN

The contractor shall configure, operate and maintain the SN infrastructure located at XXX IAW DoD and agency requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 11.0 Dedicated Customer System Support

22.4 TC

The contractor shall configure, operate and maintain the Targets and Countermeasures (TC) M&S infrastructure at XXX IAW DoD and MDA requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 11.0 Dedicated Customer System Support

22.5 IP

The contractor shall configure, operate and maintain the isolated infrastructure in conjunction with Israeli Missile Defense Office (IMDO).at CONUS sites HQ, HSV, and COS, and OCONUS sites primarily located in Israel, including the U.S. Embassy Branch Office (EBO) in Tel Aviv IAW DoD, MDA, and Israeli.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 11.0 Dedicated Customer System Support

22.6 VIPC

The contractor shall configure, operate and maintain the VIPC specialized equipment and infrastructure located at HSV IAW DoD and Agency requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 11.0 Dedicated Customer System Support

23.0 Dedicated Customer Support (Customer Funded)

(Firm Fixed Price)

The contractor shall provide comprehensive IT Service to meet end-user requirements at non-principal sites. Responsibilities include installing, configuring, maintaining, and troubleshooting systems, peripherals, and software. The technician will validate that user environments comply with Agency and DoD security standards and are maintained in alignment with operational requirements. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

Standards:

- Provide Premium Support Services IAW 11.1.1 IT Services for Premium Users
- Provide COMSEC support IAW 13.0 COMSEC Services.

- Monitor workload and trending data to validate the level of support is consistent with the demand and performance metrics requested.
- Provide all Tier II and III functions, including server and infrastructure management services, cable plant and property management, and satisfying all Agency end user immediate needs.
- Coordinate break/fix actions with the base for services provided by the host base.
- Provide onsite support for missions and mission viewings in their areas, as well as overflow support.
- Provide full-scope IPTV and VTC connectivity (e.g., LAN connections), support, operation, troubleshooting, scheduling, and use.
- Provide end-user training on common IT systems, software applications, and cybersecurity best practices, ensuring personnel are capable of utilizing the tools necessary to perform their duties effectively.

23.1 AB

The contractor shall provide multi-disciplinary personnel to configure, operate and maintain to the enterprise services extended at Pacific Missile Range Facility (PMRF) IAW DoD and Agency requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 22.0 Dedicated Customer Support

23.2 GM

The contractor shall provide multi-disciplinary personnel to configure, operate and maintain to the enterprise services extended at FGA, CLEAR AFB, Shemya, and VSFB IAW DoD and MDA requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 22.0 Dedicated Customer Support

23.3 DG

The contractor shall provide multi-disciplinary personnel to configure, operate and maintain to the enterprise services extended at Guam IAW DoD and agency requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with PWS, 22.0 Dedicated Customer Support

23.4 DV

The contractor shall provide multi-disciplinary personnel to configure, operate and maintain to the enterprise services extended at KAFB IAW DoD and MDA requirements.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 22.0 Dedicated Customer Support

24.0 IDDE for Two Letter Customers

(Firm Fixed Price) (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

24.1 GM IDDE

The contractor shall provide personnel with the knowledge, skills and abilities to configure, operate and maintain the data integration and engineering support for the GM IDDE integration efforts.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 19.0 Integrated Digital Data Environment (IDDE)

24.2 AB IDDE

The contractor shall configure, operate and maintain the data integration and engineering support for the AB IDDE integration efforts.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 19.0 Integrated Digital Data Environment (IDDE)

25.0 Development Security Operations (DevSecOps) for Two Letter Customers

(Cost Plus Fixed Fee)

The contractor shall maintain Enterprise scalable DevSecOps services to enable the rapid delivery of the software development lifecycle (SDLC) and system operations. The contractor shall implement Agile methodologies, automation, and continuous integration/continuous delivery (CI/CD) pipelines to accelerate software deployment while ensuring compliance with DoD and Agency cybersecurity and operational standards. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

25.1 GM DEVSECOPS

The contractor shall configure, operate and maintain Continuous Integration & Continuous Delivery (CI/CD) Pipeline, Analysis of Alternatives (AoA) within the Tier 2 and Tier 3 of the Tiered Mission Area (TMA) DevSecOps Ecosystem.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS, 17.0 Development Security Operations (DevSecOps)
- Support activities, meetings and provide a Weekly Activity Report (WAR) of supporting activities, participate in Scrum Board activities and Task Management

26.0 Cross Domain Solution Services for Two Letter Customers

(Cost Plus Fixed Fee)

The Contractor shall develop, implement, and manage Cross-Domain Solutions (CDS) throughout the entire System Lifecycle (SLC). (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

26.1 BC CDS

The contractor shall configure, operate and maintain CDS at XXX.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS 17.0 Cross Domain Solution Services.

26.2 DT CDS

The contractor shall configure, operate and maintain CDS at XXX.

Primary support hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call in support of maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

- Comply with the standards referenced in PWS 21.0 Cross Domain Solution Services

27.0 Model-Based System Engineering (MBSE) for Two Letter Customers

(Cost Plus Fixed Fee)

The contractor shall maintain the suite of tools used in of support the development and sustainment of system engineering activities. The tools shall support the integration of system requirements, design, performance, and verification across the program lifecycle. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

27.1 GM MBSE

The contractor shall configure, operate and maintain MBSE.

Primary service hours shall be 0600 - 1900 (ET), including onsite shift work and after-hour on-call for maintenance activities, events and tests, as directed, to minimize operational conflicts or schedule impacts.

Standards:

Comply with the standards referenced in PWS 18.0 Model-Based System Engineering (MBSE)

28.0 Solutions Development and Implementation for Two Letter Customers

(Cost Plus Fixed Fee)

The contractor shall provide project management, oversight, and technical expertise for the development, implementation and delivery of customized solutions that meet DoD and Agency compliance requirements throughout the system development lifecycle. (***This task will not be priced or evaluated with the RFP. This task will be negotiated during the MIOES Phase-In period when the workload associated with these requirements has been defined.)***

Standards:

- Execute requirements for customer-directed labs, facilities, or other specific requirements that are outside of the established, services or agreed-to network or computational performance levels.

- Comply with the standards referenced in PWS 10.2 Solutions Development and Implementation

AB Reserved
BC Reserved
CA Reserved
CC Reserved
CR Reserved
CS Reserved
CT Reserved
DA Reserved
DE Reserved
DG Reserved
DI Reserved
DT Reserved
DV Reserved
DW Reserved
DX Reserved
DZ Reserved
EO Reserved
GC Reserved
GM Reserved
GW Reserved
IC Reserved
IP Reserved
IR Reserved
IS Reserved
PA Reserved
QS Reserved
SB Reserved
SN Reserved
SS Reserved
TC Reserved
TF Reserved
TH Reserved