Missile Defense Agency (MDA)

MDA Information Technology Operations & Engineering Solutions (MIOES) Contract

Basic Performance Work Statement

Dec 17, 2024

1.0 Mission

1.1 The Missile Defense Agency (MDA) has a continuing need for the research, development, test, evaluation, and integration of Missile Defense System components. These activities rely heavily on MDA Information Management (IM) systems, underlying Information Technology (IT), and facility infrastructure that support rigorous Missile Defense System capability development and business operations for MDA. A Research Development Test and Evaluation (RDT&E) IT ecosystem is required to provide MDA with a secure development, test, digital engineering and modeling environment, and continuous access to unclassified and classified networks and collaboration services.

1.2 IM and underlying IT infrastructure is also critical to the daily operations of MDA personnel to collaborate across all classification domains with each other, Senior Department of Defense (DoD) and other United States (US) Government agency personnel, Combatant Commanders, North Atlantic Treaty Organization (NATO) partners, allies, and industry partners. It requires advanced and persistent cybersecurity vigilance that ensures daily operations and communications are protected and safeguarded.

1.3 These activities are conducted across MDA's worldwide enterprise and within the Missile Defense Integration & Operations Center (MDIOC) mission execution platform.

1.4 The MDA Information Technology Operations & Engineering Solutions (MIOES) contract operates within the complexities of this dynamic environment and enables MDA to simultaneously conduct Missile Defense System development, testing, warfighter training, and operations support for multiple MDA directorates and Combatant Command requirement owners while executing the MDA enterprise communications and IT mission. This contract offers a capability for government and contractor stakeholders to operate within this environment that requires a continuous, real-time, compliant, cyber secure IT and facility infrastructure capable of conducting concurrent event execution and continuous real world, 24x7x365 mission operations. The MIOES contract enables the rapid response to evolving and emerging priorities of global enterprise communications and IT, RDT&E and mission operations, and operational training in a highly cohesive and collaborative mission environment.

2.0 MIOES Scope

The work that will be executed under the MIOES contract is summarized in the following technical areas (TA):

Technical Area (TA)	Name	Description
1	**Enterprise/RDT&E IM** Global Communications & RDT&E/Enterprise Information	1. Communications Services & Solutions. Operational planning and logistics for the provisioning, development, integration, operations, management, sustainment, and interoperability of reliable communication networks. 2. Enterprise Services & Solutions. Services, solutions and end-user support required to manage MDA's globally dispersed network that can

	Management (IM) Solutions & Integrated Architectures	simultaneously support Missile Defense System RDT&E systems and operations. 3. System Architecture Solutions. Development of technical baselines and reference architectures for standard designs and solutions. 4. Mission Assurance and Configuration Management. Governance to establish and sustain effective operations, architectures, solutions, processes. 5. Cybersecurity. Provide Defensive Cyberspace Operations and robust cybersecurity solutions to protect and defend the Missile Defense System
2	**Mission IM** Missile Defense System Mission & Event Operations: IM Architectures & Solutions	1. Design, develop, integrate, operate, and sustain secure and reliable IM architectures and IT infrastructure, for mission systems enabling a continuous operational readiness posture. • C2BMC mission laboratories and enclaves • Ground-Based Midcourse Defense Operations and Training Center • Ballistic Missile Defense System Network Operations and Security Center • Operations Support Center • Missile Defense Space Enterprise Architecture • MDA Enterprise Ground Services • Space Test and Integration Laboratory • Missile Defense Space Operations Center • Engineering Web Services and Modeling and Simulation Center • JFCC-IMD Operations Center 2. Conduct Missile Defense technology maturation, design, development, prototyping, demonstration and testing.
3	**MDIOC Facility Operations** MDIOC Operations, Sustainment, Restoration & Modernization	1. Operate and maintain the MDIOC facility infrastructure. • Sustainment: maintenance/ repair activities • Restoration: restoring real property to its designated purpose • Modernization: alteration/replacement of facilities solely to implement new or higher standards, to accommodate new functions, or replace building components
4	**MDIOC Integration** MDIOC Planning and Integration	1. Planning and integration to ensure MIOES activities do not interfere with real-world Missile Defense System mission and exercise/test events performed within or supported by the MDIOC range. 2. Develop and execute mission assurance and configuration management practices and alignment to ensure MIOES activities are validated, aligned and integrated with MDIOC standards and processes. 3. Develop, implement, and deliver a MDIOC Range Integrated Schedule • MDIOC activities, facility infrastructure and maintenance projects, network modifications/projects 4. Develop and maintain the MDIOC facility infrastructure technical baseline. 5. Establish event configuration protections for mission and test assets to prevent unapproved access/changes through physical and logical seals & access restrictions.

A significant requirement of this dynamic environment is the interface, leadership, and management necessary to integrate between all technical areas. Simultaneous events compounded with concurrent research, development, test, and operations compete for both physical assets and personnel resources. This integration and deconfliction requires coordination and resource prioritization to accommodate event schedule changes, facility or IT system changes, test article improvements, and contingency operations. This environment requires the synchronization of capabilities, schedules, and priorities across the program.

3.0 MIOES Requirements (Technical Areas 1 – 4)

3.1 Global Communications & RDT&E/Enterprise Information Management (IM) Solutions & Integrated Architectures

3.1.1 Develop, upgrade, operate, and maintain an RDT&E/Enterprise worldwide IM/IT ecosystem that provides MDA with a secure development, test, digital engineering and modeling environment. This environment serves as the integration point which facilitates the rapid development and delivery of Missile Defense System capabilities and becomes the RDT&E resource for daily operations that includes data analytical decision making, test events and capability delivery to the Warfighter. (Note: for purposes of clarification for the RFP, data analytical decision making is referring to IT service delivery and it's asscociated communication architectures vice "post mission" data analysis. It should be noted that network analysis is imperative to provide ontime trusted data delivery back to the Data Centers or service delivery point(s) of the supported stakeholder. This note will be deleted at time of contract award.)

3.1.2 Provide information handling; processing, storage, monitoring, and transport. Perform systems and network management; information dissemination management; and cybersecurity (technical & management) functions. Provide MDA with secure environment to include classified and unclassified IT systems, cloud and data centers, operations and monitoring centers, telecommunications, local and wide-area network infrastructures; and customer services while maintaining an integrated and comprehensive cybersecurity capability across IT systems, enclaves, and networks.

3.1.3 Provide effective, efficient, secure, and reliable information network services for critical DoD and MDA communications and information processing integrating accepted industry best practices that align/meet DoD compliance requirements.

3.1.4 Provide cybersecurity assurance by utilizing risk management framework (RMF) to establish and maintain security standards and guidance to promote the development of comprehensive and balanced information security programs

3.1.5 Utilize a cloud first strategy that enables cloud computing on-demand access, via secure network connectivity, to deliver global IT services to the warfighter and general user base.

3.1.6 Maintain an IT as-a-service (ITaaS) capability. Enable the MDA Cloud capabilities to provide on-demand network access to a shared pool of configurable computing resources

which can be rapidly provisioned and released. Automate the provisioning of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS).

3.1.7 Manage two major data centers (Huntsville, AL and Colorado Springs, CO) that provide a mix of classified and unclassified IT services, with each providing disaster recovery and continuity of operations for critical services to the other.

3.1.8 Collaboration across multifunctional teams to formulate, plan, implement, manage, track, and evaluate large scale/complex IT architecture/systems projects with an agile approach to rapidly deliver capabilities to the customers. Application of creative and integrated solutions-based thinking to spark enduring change and adopt innovative solutions into the Enterprise.

3.1.9 Perform Tier III Cybersecurity Roles and Functions services across the entire portfolio of systems to foster an integrated Cybersecurity Management that drives a holistic and collaborative cyberspace program dedicated to delivering a secure and uncompromised Missile Defense System through innovative and optimized cyber resilient initiatives focused on continuously improving MDA cyber capabilities, risk-level, and mission survivability.

3.1.10 Analyze, investigate, respond to, and report cyber incidents. Use threat hunting tools to identify cybersecurity risk to MDA Enterprise and RDT&E IT Systems. Monitor MDA cyber terrain and report to DoD. Provide Tier II cybersecurity services.

3.1.11 Perform Global lifecycle event management, engineering services, and support for MDA Missile Test Events, Mission/Real World Events, Flight Tests, Ground Tests, Wargames/Exercises, Experiments, and Continuous Developmental Integration (CDI) activities. Includes missile test event requirements management, coordination, planning, architecture development, service solutions, execution support, resource management, asset management, work activity de-confliction. Planning, integration, and execution for all IT requirements/communications in support of flight test, ground test, wargames and exercises, real world missile test events, and CDI.

3.1.12 Architectural design, development, and integration of an Enterprise-wide ecosystem of digitally transformative technologies that provide rapid, continuous innovation, increased resiliency, more efficient processes and workflows, and increased cyber security. This ecosystem is the backbone on which all required capabilities are accessed by stakeholders using a federated multi-tenant model. This ecosystem must support the parallel operation of enterprise level capabilities and 24x7x365 RDT&E related capabilities.

3.1.13 Positioning, Navigation and Timing (PNT) Resiliency Enhancements. Provide PNT enhancements to improve PNT assurance posture for the Missile Defense System. Provide improved architectural delivery of time and frequency signals to the Missile Defense System elements through testing and analyses associated with incremental improvements as they become available technologically and programmatically. Manage coordination with PNT stakeholders and stay abreast of advancements in PNT threats and capabilities. Integrate with other related

agency and warfighter activities and missions to capture interface management, process implementation, and lifecycle management of the PNT enhancements deployed.

3.1.14 Provide the MDA Foreign Military Sales (FMS) office with IT administrative and equipment, capabilities and services to MDA personnel supporting security assistance and MDA FMS activities.

3.1.15 Develop, maintain, and execute an enterprise common-use IT architecture program and establish governance to develop common-use IT technical baseline standards to include records asset ownership, accountability, and traceability of requirements, architectures, and engineering baselines. Develop technical baseline standards for common-use IT systems and services. Mature the common-use IT technical baseline and ensure standardized governance to engineers, developers, project/systems engineers, and solution architects. Establish technical baseline repository standards for historical artifacts, the provenance of those artifacts, and supporting data.

3.1.16 Develop, maintain, and execute an enterprise common-core IT Mission Assurance (MA) program providing a disciplined application of systems engineering, risk management, quality, and management principles to achieve success of IT systems design, development, testing, deployment, and operations.

3.1.17 Develop, maintain, and execute an enterprise common-core IT Configuration Management (CM) program to manage and account for consistency, continuity, and the integrity of configured common core IT items and systems. Develop and maintain a technical baseline (Requirements Baseline, Architectural Baseline, and Engineering Baseline) to ensure system configurations are documented and accurately reflect the environment and map ownership of systems to ensure timely information can be provided to impacted stakeholders.

3.2 Missile Defense System Mission & Event Operations: IM Architectures & Solutions

3.2.1 The MDIOC is host to numerous Missile Defense System operational missions (e.g., Command, Control, Battle Management, and Communications (C2BMC), 100th Missile Defense Brigade (MDB), Joint Functional Component Command for Integrated Missile Defense (JFCC-IMD)), as well as operational test assets (e.g., satellites). Mission IM support, solutions, architecture, design, and engineering must be provided in a manner to maintain an operational readiness posture in order to deliver warfighter mission support and execute the Missile Defense System mission. Develop, implement, integrate, operate, mature, and sustain secure and reliable architectures and an IM infrastructure, while ensuring the following:

- Heightened level of responsiveness and the mission assurance rigor to ensure availability of operational Missile Defense System assets
- Continuous situational awareness and mission assurance support (24/7/365) as well as the ability to escalate health and status issues of critical infrastructure resources that directly support the operational Missile Defense System assets
- Increased responsiveness and mature, technical governance to enable full operation
- Mandated hardware, software, interfaces, and configurations

3.2.2 Conduct Missile Defense requirements analysis, concept exploration, technology maturation, design, development, prototyping, demonstration and testing.

3.2.3 Ensure an integrated, repeatable, scalable, and interoperable IM framework in optimizing agile and secure capabilities to meet mission requirements, maintain full spectrum cyber security resilient capabilities and maintain pace with technological advancements for the following Missile Defense System mission enclaves:

- Ballistic Missile Defense System Network Operations and Security Center (BNOSC)
- Ground-Based Midcourse Defense (GMD) Operations and Training Center
- C2BMC mission laboratories and enclaves
- JFCC-IMD Operations Center
- Operations Support Center
- Missile Defense Space Enterprise Architecture (MDSEA)
- Space Test and Integration Laboratory
- Missile Defense Space Operations Center (MDSOC)
- Engineering Web Services (EWS) enclave and the Modeling and Simulation (M&S) Center
- Simulation Interface Unit (SIU) hardware, software, and material

3.3 MDIOC Facility Operations & Sustainment

The MDIOC is a secure, 4-story, multi-purpose and highly reconfigurable 676,160 square foot research, test, and operations complex comprised of two separate facilities. These facilities reside within the Space Base Delta 1 restricted area on Schriever Space Force Base, CO.

3.3.1 MDIOC Facility Operations. Operate, and maintain an efficient, cost effective facility infrastructure in support of MDA elements / components and designated Combatant Commanders' Missile Defense System operations executing missions at the MDIOC. Provide a reliable infrastructure supporting mission-critical Missile Defense System activities as well as a clean, safe, and environmentally responsible infrastructure. Provide a safe and reliable building infrastructure. Maintain a high level of appearance standards. Provide emergency infrastructure to support operations during contingencies. Execute a preventative maintenance program.

3.3.2 MDIOC Facility Restoration and Modernization. Facility sustainment, restoration, reconfiguration, and modernization projects required to support MDA mission activities within the MDIOC and its area of responsibility. Provides facility engineering solutions to plan, design, execute and transition of improved or modified facility architectures and infrastructure systems. Management and execution of facility modifications and restoration. Maintain positive configuration control and documentation of facility restoration and modernization activities.

3.3.3 Supply Chain Operations. Perform supply chain operations in Colorado Springs, Huntsville, and Fort Belvoir areas in government provided facilities that includes warehouse and

receiving area operations such as inspection and acceptance, packaging, shipping, receiving, ground handling, storage, distribution, transportation and inventory management.

3.4. MDIOC Planning, Integration, Operations

3.4.1 Process Development

3.4.1.1 Develop processes to ensure MDIOC facility mission assurance and configuration management for facility projects that will be executed under the MIOES contract. Ensure processes are integrated with each other and align with the MDIOC level plans (e.g., MDIOC Systems Engineering Plan, MDIOC Mission Assurance Plan, MDIOC Configuration Management Plan). Develop processes that ensure MIOES activities impacting the MDIOC facility are validated, align with facility standards, and solutions are integrated across the MDIOC facility through the MDIOC Engineering Review Board.

3.4.1.2 Develop processes to establish how change occurs to the MDIOC facility technical baseline. Develop standards that can determine which baselines are impacted by a stakeholder requirement and the process to update controlled baseline artifacts as a result of that requirement. Identify and track configuration items through the defined engineering lifecycle to ensure a low risk posture to the MDIOC Range.

3.4.2 Event Situational Awareness Development

Develop, implement, and deliver a time-phased MDIOC Range Integrated Schedule that includes Concurrent Test and Training Operations (CTTO) activities, facility infrastructure and maintenance projects, major network modifications/projects, and base projects with potential to impact MDIOC range activities.

3.4.3 Operations Assessment Development

Monitor integrated planning and operations that will enable effective and efficient ongoing integrated planning and operations activities across the MDIOC range. The method generated will be based upon key priorities for ensuring risk mitigation for any impacts to the MDIOC.

3.4.4 MDIOC Facility Mission Assurance

3.4.4.1 Champion all requirements through the MDIOC Facility Boards (e.g. Engineering Review Board, Configuration Control Board, Range Risk Board, Range Outage Board) by coordinating and communicating the MIDIOC facility standards, board artifact submission requirements, and actions required under each board charter with those stakeholders who will be presenting at the MDIOC boards. Identify, track, and resolve issues.

3.4.4.2 Maintain the MDIOC facility technical baseline to ensure facility system configurations are documented to accurately reflect the environment and map ownership of systems to ensure provision of timely information to impacted stakeholders. The technical baseline consists of Requirements Baseline, Architectural Baseline, Engineering Baseline.

3.4.5 Event Protection

3.4.5.1 Establish event configuration protections for mission and test assets through physical and logical seals and access restrictions to prevent unapproved access or changes. Coordinate and communicate planned and emergent MDIOC range outages, incidents, issues and concerns, communicate mission impacts and the ongoing activities to restore normal conditions.

3.4.5.2 Facilitate government review and approval of work during Event Protection Periods (EPPs) to prevent adverse impacts to flight/ground test events and wargame/exercise execution. Participate in the MDIOC Range Work Screening Team during EPPs to review and authorize physical/logical work taking place in the MDIOC range to prevent mission and event impacts from occurring.

3.5 Contract Leadership & Management

3.5.1 Provide collaborative, flexible, and responsive leadership and management to innovate, set standards and goals and execute and control all activities across the MIOES contract. Provide workload capacity planning, monitoring, coordination, and integration and program integration that results in a consistent requirements execution methodology and mission assurance.

3.5.2 Plan, integrate, coordinate, communicate, and manage cost, schedule, and performance, to enable disciplined work performance, technical direction, surveillance, resource application, reporting and the management of requirements, resources, business systems, and data.

3.5.3 Provide collaborative and agile program integration required to innovate and establish MIOES contract-wide, enterprise standards to execute seamlessly all activities across the MIOES contract.

3.6 Business Planning

3.6.1 Define, coordinate, and develop plans to coordinate, integrate, and align all activities, projects, and solutions across the MIOES contract.

3.6.2 Develop overarching processes to ensure MIOES activities, projects, solutions are validated and aligned and adhere to established engineering principles, processes, architectures, baselines, MDA test and event governance, and MDIOC facility standards.

3.6.3 Develop methods to monitor and surveil MIOES integrated planning and operations that enables the government and contractor to evaluate the effectiveness and efficiency of ongoing integrated management, planning and operations activities across the MIOES contract.

3.7 Business Controls

3.7.1 Monitor, measure, control, and report contract cost, schedule, and performance metrics

4.0 Other Requirements

4.1 Provide a workforce capable of handling, processing, and protecting critical unclassified information and classified information in accordance with DoD, MDA, Program, and mission/event specific security requirements. Comply with the security requirements and mission/system specific security requirements outlined in the DD 254. Comply with the Information Management and Control Plan.

4.2 Develop, implement, and maintain a procurement and government property control program that ensures compliance with Federal, DoD, and MDA directives and policy for the procurement, tracking and management of Government Property, Government Furnished Property and Contractor Acquired Property. Property to include consumables, equipment, hardware, and software. Government property necessary for accomplishment of requirements will be identified within individual task orders.

4.3 Develop and execute supply chain risk management practices in order to identify supply chain vulnerabilities, threats, and potential disruptions and implement mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services.

4.4 Develop and execute information security, personnel, operations, physical, export control, and cybersecurity controls and processes in accordance with Federal, DoD, and MDA regulations, policies, procedures, standards.

4.5 Comply with applicable federal, state, and local Environmental Safety and Health laws and regulations, Executive Orders, and policies in all phases of program execution.

4.6 Develop, implement, and maintain systems engineering, mission assurance, configuration management, enterprise architecture, quality assurance, risk management programs.

4.7 Comply with the MIOES Performance Evaluation and Incentive Plan as tailored in each task order PWS.

4.8 Delivery of all Contract Data Requirements List (CDRL) products as instructed in each task order PWS.

4.9 Research, procure, develop, integrate and perform continuous monitoring/assessment of risk adverse products and solutions to support the MDA's requirements. This includes designing, building, securing, operating, defending and protecting MDA resources. This shall include the skills and knowledge required to build and maintain a comprehensive cyber resilient program that incorporates zero trust principles, ensuring the systems uphold the highest level DoD and MDA cybersecurity compliance standards throughout the lifecycle of each program.

4.9.1 Identify, manage, verify, and validate Cybersecurity requirements in the same manner as all other program requirements;

4.9.2 Integrate Cybersecurity considerations into program systems engineering and design processes.

4.9.3 Provide support, source data, and analysis required to support the Government in obtaining system authorization in accordance with DoD Instruction 8510.01, Risk Management Framework (RMF).

4.9.4 Provide support, analysis of the MDA Cybersecurity insider threat program, computer network defense support program, and RMF efforts within the supported programs.

4.10 Directives/regulations that are applicable to all task orders are identified in Attachment 3, Compliance Documents. Tailoring, as necessary, may be done at the task order level.

5.0 Telework and Remote Work

5.1 Telework

5.1.1 Routine Telework. Work performed at an alternate work located no further than 50 miles from the Government facility on a regular/recurring basis unless specifically prohibited in the Performance Work Statement (PWS). Example when this may be appropriate are when the requiring activity determines a function can be performed at a non-Government provided location and/or when workspace at the Government facility is unavailable and the functions can be performed via a telework arrangement with "as required" access to the Government facilities, e.g., hoteling workspace, required meetings, etc.

5.1.2 Situational Telework. Situational is an arrangement where the employee performs work at the primary office worksite. Telework is only approved on a short-term basis for good cause. Examples of situations when situational telework may be appropriate are when an employee needs to complete discrete portions of projects or work assignments, recovery from a short-term illness and/or injury, when office space is unavailable due to renovations, or when OPM announces the Federal Government operating status, in the area of the Contractor's regular worksite as, "Open with an Option for Unscheduled Telework."

5.1.3 Remote Work. Remote work is an arrangement that allows the contractor employee to perform work during any part of regular, paid hour, at an alternative worksite located more than 50 miles from the identified Government facility as stated in Performance Work Statement (PWS). Remote Work is authorized when it meets PWS requirements or contract terms and conditions unless specifically prohibited in the PWS. The Contractor is wholly responsible for its employees and shall ensure that they are productive and are in compliance with security and safety requirements during remote

work. Remote work must be supported by an advantageous business case analysis coordinated with and approved by the requiring activity and IS Program Office. The Government reserves the right to modify, in whole or in part, or terminate, in whole or in part, any remote work authorization, if it is determined to be in the Government's interest. The Contracting Officer will provide written notice of modification or termination with specifics 30 days prior to the anticipated effective date. There shall be no increased cost to the Government for remote work.

5.1.4 In cases where the Government authorizes an alternate location, equivalent workstation and collaboration/communication equipment that would normally be provided in a Government-provided location will be furnished to the Contractor as Government Furnished Property. The Contractor assumes, until such time it is returned, responsibility for the equipment once it is assigned to its employees. The Contractor and/or its employee acknowledges receipt of the property with the closure of the MDA Kinetic Service Request (KSR). The Government will continue to provide network connection via VPN and technical support for the equipment provided. The Government will not provide internet connectivity for Contractor employees. Upon contract award, a copy of the contractor's remote work policies and a sample employee agreement shall be submitted to the Contracting Officer for review.

6.0 Predominate MDA Facilities

6.1 Schriever SFB, CO and MDIOC

Access to Schriever SFB (SSFB) is strictly controlled; to access the installation requires a sponsorship by a person assigned/employed on the installation for personnel who do not possess some form of current federal government issued identification. The MDIOC is located within a USAF restricted area on SSFB, contractor employees require at a minimum a National Agency Check Investigation (NACI) and a Visit Authorization Request (VAR) for issuance of a temporary or permanent badge that allows unescorted access to the restricted area.
In order to qualify for issuance of a Restricted Area Badge/Automated Entry Control Card, the respective member must physically enter the Restricted Area once a week for at least a 90-day increment to perform official duties that warrant unescorted entry authorization, and at least once a week entry into the RA after the 90-day period has surpassed. The Commander may grant individuals access to the Restricted Area after the following has been completed: 1) the contractor completes the Standard Form (SF) 85P and it is submitted to Office of Personnel Management (OPM) for a National Agency Check Investigation (NACI); 2) a check of the Defense Clearance and Investigation Index (DCII) reveals no relevant, significant information which might preclude unescorted access; and 3) a check of the appropriate local records has been accomplished. Since access to the MDIOC is controlled, it is important to understand the potential impacts to the contractor(s) ability to accommodate/respond to requirement fluctuations (e.g., surge support, competing/overlapping schedules, etc.); this potential impact must be considered in all proposed solutions.

6.2 Redstone Arsenal, AL and MDA Controlled Space(s).

To gain access to Redstone Arsenal, a VAR is required and needs to be approved by a Government POC in order to gain access. If an individual meets the criteria and they have a CAC, then a MDA form 10 signed by their Government POC or security manager will be needed to enroll them into our access control system.

A CAC is required to access Redstone Arsenal. Individuals that don't have a CAC can have their Government POC send a request to the Redstone Visitor Center so the individual can gain access. Contact MDA Security Operations Center for information and procedures pertaining to MDA controlled space(s).

6.3 Fort Greely, AK and Missile Defense Complex Restricted Area.

Access to Fort Greely Army Garrison (FGA) is a Closed Post; contractor employees must have a local government sponsor and will be required to pass a National Crime Information Center (NCIC) Criminal Background Check review prior to unescorted entry. Contractor employees that possess at least an interim Secret security clearance will not be required to submit an NCIC criminal background check. Procedures and information pertaining to access is available by contacting the Fort Greely Installation Visitor Control Center. Additionally, the Missile Defense Complex (MDC) is a designated restricted area on FGA. Contractor employees requiring unescorted entry to the MDC must have an approved VAR on file, possess an interim Secret security clearance at a minimum and have local government approval. Contact MDA/GMF (Ground-based Midcourse Defense Operations Support at FGA) Security Manager at for additional information on FGA restricted/control area access requirements.

6.4 Vandenberg SFB, CA and Restricted Areas containing Ground-based Midcourse Defense (GMD) assets.

6.4.1 Vandenberg SFB: Personnel who do not possess some form of current federal government issued identification to access the installation, and those who do not possess a need to enter the installation on a regular basis require sponsorship by a person assigned to or employed on the installation. Contact your sponsor or the Security Forces Visitor Control Center for procedures and information pertaining to installation access.

6.4.2 Vandenberg SFB Restricted Areas: Additionally, there are restricted areas on Vandenberg SFB that contain MDA resources. Contractors are required at a minimum a National Agency Check Investigation (NACI) for unescorted access to the restricted area(s). Contractors operating 90 consecutive days may be issued a permanent Restricted Area badge for unescorted access to the GMD site; terms will apply badges stay at VSFB with Security POC. Commanders or Equivalent may grant individuals access to the Restricted Area after the following has been completed: 1) completion of the Standard Form (SF) 85P and it is submitted to Office of Personnel Management (OPM) for a National Agency Check Investigation (NACI); 2) a check of the Defense Clearance and Investigation Index (DCII) reveals no relevant, significant information which might preclude unescorted access; and 3) a check of the appropriate local records has been accomplished. Since access to the GMD operational areas are restricted, it is important to understand the potential impacts to the contractor(s) ability to accommodate/respond to requirement fluctuations (e.g., surge support, competing/overlapping

schedules, etc.); this potential impact must be considered in all proposed solutions. Contact Security Forces at 805-606-1853 for procedures and information pertaining to restricted area access.

6.5 Naval Support Facility-Dahlgren, VA and MDA Controlled Space(s).

Access to Dahlgren is strictly controlled; to access the installation requires a visit request sponsored by a person assigned/employed on the installation at the Pass & Identification (ID) center for personnel who do not possess some form of current federal government issued identification. A picture ID is required prior to the issuance of guest badge and a temporary car pass from the Pass & ID center for installation access. Contact the Dahlgren Visitor Control Office for procedures and information pertaining to installation access. MDA facilities are controlled areas and require an approved Visitor Access Request (VAR) or an enrolled DOD CAC to gain unescorted entrance to any of the facilities. Unescorted access is granted to cleared MDA personnel and contractors and to other persons who, in the course of official business, have a current security clearance on file, a need to conduct MDA business, and have a need to know. Contract personnel are approved for access through CORs and Security Managers; their issued DOD CACs are then enrolled for building access. Contact MDA Dahlgren Security Operations Center for information and procedures pertaining to MDA controlled space(s).

6.6 Ft. Belvoir, VA and MDA Headquarters Command Center.

Access to Ft. Belvoir is strictly controlled; to access the post requires personnel with a legitimate need, but without some form of current federal government issued identification, to stop at the visitor center and complete paperwork for a temporary access pass. Contact the US Army Garrison, Ft. Belvoir visitor center for information and procedures pertaining to post access. MDA Headquarters Command Center (HQCC) is a controlled area facility and requires an approved VAR or an enrolled DOD CAC to gain unescorted access. Unescorted access is granted to cleared MDA personnel and contractors and to other persons who, in the course of official business, have a current security clearance on file, a need to conduct MDA business, and have a need to know. Contract personnel are approved for access through CORs and Security Managers; their issued DOD CACs are then enrolled for building access. Contact MDA HQCC Security Operations Center for information and procedures pertaining to MDA controlled space(s).

6.7 Pacific Missile Range Facility and Aegis Facility Access.

Access to Pacific Missile Range Facility (PMRF) is controlled; to access the installation requires a sponsorship by a person assigned/employed on the installation for personnel who do not possess some form of current federal government issued identification. It is strongly recommended you contact the Security Pass & ID Office for procedures and information pertaining to installation access. Due to the geographical location of PMRF MDA, contractors supporting missions at that location will require prior Government approval for travel due to limited supporting resources. Each visit requires an MDA PMRF Arrival/Departure (A/D) Form -send an unencrypted email to pmrfarrival-departure@mda.mil to request a form.

6.8 Outside the United States, Puerto Rico, U.S. possessions and trust territories.

Performance will occur at various MDA and/or other government locations as directed by the Performance Work Statement. The contractor shall abide by government security requirements

per NISPOM Chapter 6 The cognizant security office at the performance location is MDA or the host installation.

Attachment 1
Performance Work Statement (PWS) Task 8.1

Background:

Under the current IRES contract, Task Order 8002 includes IRES Program Management and Program Integration for the overarching contract level requirements. This task is traditionally where more senior level program and functional leaders charge their time against contract level requirements that are applicable to all task orders. It represents work that is not easily severable between task orders or would be burdensome to charge multiple increments of time against multiple task orders. This same task order also has a requirement for MDIOC Mission Engineering.

Under the MIOES contract, there will not be a single task order for the MIOES Program Management and Integration tasks. Instead, the contractor shall create an "overhead/indirect" type account that collects these costs that can then be charged against each task order. Under MIOES there will still be a single task order for Mission Engineering requirements.

The PWS language below represents the MIOES Program Management and Integration requirements which will be documented in the Basic PWS and referenced as a task in the PWS for each task order. This task will be identified as 8.1 under each task order and costs shall be allocated to each individual task order.

The Government will have a separate Contracting Officer Technical Representative that will provide technical oversight and surveillance against this task. In additiona, a separate, single Status Report will be required to report the performance, cost, schedule status of this task.

Contract Data Requirements List (CDRL) Requirements:

Task	CDRL	DID	Title
8.1.1.3	A8.1.01	DI-MGMT-80004	Management Plan
8.1.1.7	A8.1.02	DI-MGMT-80368A	Status Report
8.1.2.2	A8.1.03	DI-MGMT-81861	Contract Summary IPMDAR – Cost Only - DFARS EVMS not applicable
8.1.2.3	A8.1.04	DI-FNCL-81765C	Contractor Business Data Report—CCDR DD Form 1921-3
8.1.2.3	A8.1.05	DI-MGMT-82164	Quantity Data Report—Flexfile Contractor Cost Data Report (CCDR)
8.1.2.3	A8.1.06	DI-FNCL-82162	Cost and Hour Report (Flexfile) -- CCDR)
8.1.2.13	A8.1.07	DI-MGMT-1334D	Contract Work Breakdown Structure (CWBS)
8.1.2.14	A8.1.08	DI-MGMT-81468A	Contract Funds Status Report (CFSR)
8.1.9.2	A8.1.09	DI-MGMT-82256	Supply Chain Risk Management Plan
8.1.10.1	A8.1.10	DI-MGMT-82041B	Small Business Participation Report
8.1.12.1.	A8.1.11	DI-MGMT-82383	Information Management and Control Plan (IMCP)
8.1.13.1	A8.1.12	DI-MISC-80508B	MIOES Contract Phase-Out Plan

8.1 MIOES Contract Level Management

8.1.1 Program Management and Leadership

The contractor shall plan, integrate, coordinate, communicate, and manage cost, schedule, performance, and risk to enable disciplined work performance, technical direction, surveillance, resource application, reporting and the management of requirements, resources, business systems, and data.

Standards:

8.1.1.1 Perform functions required to ensure proactive and sustained operational excellence in providing accurate, safe, secure, timely, program integration across all applicable Task Orders (TOs) to deliver capabilities and solutions.

8.1.1.2 Provide a Program Manager (PM) with authority to act on behalf of the entire contractor team that has local autonomy and full authority to commit the corporate resources to execute the MIOES contract.

8.1.1.3 Deliver a MIOES Management Plan and manage all activities within the plan. (CDRL A8.1.01).

8.1.1.4 Manage Portfolio/Project Management practices in a way that enables technical consistency and cost effectiveness while providing an adaptable framework for planning, managing, and completing projects for a broad range of tasks and missions.

8.1.1.5 Adjust processes and resources in balancing risks and opportunities.

8.1.1.6 Implement tools, training, and processes that will foster sustainable innovation into daily operations that will improve effectiveness and efficiencies and reduce costs in a resource-constrained environment, while minimizing risk.

8.1.1.7 Deliver a Task 8.1 Status Report for all PWS paragraph 8.1 activities that reports integration efforts, status, accomplishments, and issues to promote full and transparent communications (8.1 activites shall not be reported in the individual task order status reports) (CDRL A8.1.02).

8.1.1.8 Mitigate workforce surge and draw-down impacts by analyzing workforce trends, forecasting workforce needs, and hiring to those requirements.

8.1.1.9 Maintain a qualified workforce as demonstrated by training and skills certification, engineering and operations workforce experience, educational attainments and security clearances.

8.1.1.10 In–process and out-process employees in the Program Resource Internet Database Environment (PRIDE) Workforce Integration Tracking system (WITS) in accordance with MDA 1400.07-INS.

8.1.1.11 Complete the MDA Form 14 –Out-Processing Checklist, as required by MDA Instruction 1400.07-INS, and return the completed checklist, with all required signatures, to the cognizant Contracting Officer's Representative (COR) prior to the departure of the employee.

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

8.1.1.13 Implement all business systems in accordance with DCAA and DCMA directives and participate in business system reviews and correct deficiencies as defined in the findings.

8.1.1.14 Prepare for and participate in mandated audits, such as Inspector General, Cyber Operational Readiness Assessment, physical security, environmental and safety, and property.
8.1.1.15 Comply with Workplace Next manpower allocations for on-site and telework positions.

8.1.2 Measurement and Control

The contractor shall monitor, measure, control, and report contract cost, schedule, and performance metrics

Standards:

8.1.2.1 Implement and administer a compliant Earned Value Management System (EVMS) for utilization on all applicable TOs.
8.1.2.2 Deliver a MIOES-level Integrated Program Management Data and Analysis Report (IPMDAR (Contract Summary IPMDAR – Cost Only) (CDRL A8.1.03).
8.1.2.3 Systematically collect and report actual contract costs segregated by non-recurring and recurring, functional category, and by unit and/or lot as designated by the government provided Cost Data Summary Report (CSDR) Plan (DD Form 2794) (Reference Attachment 5), (CDRL A8.1.04, Contractor Business Data Report—CCDR DD Form 1921-3, CDRL A8.1.05, Quantity Data Report—Flexfile Contractor Cost Data Report (CCDR), CDRL A8.1.06, Cost and Hour Report (Flexfile) -- CCDR).
8.1.2.4 Provide one report at the IDIQ level that includes all costs of all task orders represented as Order/Lot IDs.
8.1.2.5 Provide a list of all subcontractors on the contract in a resource distribution table as outlined in the CDRL.
8.1.2.6 Notify the Government of all subcontractors expected to have a contract value greater than $20M over the life of their subcontract as outlined in the CDRL
8.1.2.7 Flow down requirements contained from the prime contract to the subcontractors as outlined in the CDRL.
8.1.2.8 Include the subcontractor's submission with the prime contractor's submission (prime contractor submission will not be evaluated without the subcontractor submission).
8.1.2.9 Participate in a CSDR Readiness Review which finalizes the contractor's CSDR process to satisfy the guidelines contained in the DoD 5000.04-M, CSDR Manual, and the requirements in the CSDR plan.
8.1.2.10 Accept or propose changes to expand the Government-provided preliminary WBS as provided in the CSDR Plan to represent how the contractor plans to accomplish the contract scope of work consistent with the contractor's internal organization and processes.
8.1.2.11 Participate (prime and subcontractor) in a semi-annual Common Cost Methodology Working Group (CWG) as described in MDA Directive 4250.02 – Missile
8.1.2.12 Defense System Cost Estimating and perform cost estimating analysis in accordance with the MDA Cost Estimating and Analysis Handbook, and provide data to support the CWG.
8.1.2.13 Deliver a Contract Work Breakdown Structure (CWBS) (CDRL A8.1.07).
8.1.2.14 Deliver a Contract Funds Status Report (CFSR) (CDRL A8.1.08)

8.1.3 Program Integration.

The contractor shall provide comprehensive and enforceable, collaborative and agile program integration required to establish enterprise level standards, for non-mission systems and networks, in order to seamlessly execute all activities across the MIOES contract.

Standards:

8.1.3.1 Implement program integration elements that enable the integration of people, processes, and tools that aligns capabilities, resources, schedules, and priorities across the contract.

8.1.3.2 Plan, schedule, organize, and report on internal process audits and evaluate organizational processes at the enterprise level and across TOs that drive integration across the contract.

8.1.3.3 Capture and maintain data to enable schedule integration and forecasting of activities across the contract.

8.1.3.4 Discover, manage, and communicate dependencies and potential impacts to critical path activities across all appropriate stakeholders and develop Courses of Action and mitigation strategies for government approval.

8.1.3.5 Comply with the MDA and MDIOC Facility Systems Engineering Plans (SEP) across all task orders.

8.1.3.6 Report Program Integration successes, challenges, and gaps in the Task 8.1 Status Report.

8.1.4 Enterprise Planning and Governance

The contractor shall perform planning and governance to coordinate, integrate, and align activities, processes, projects, and solutions across the MIOES contract. The contractor shall follow a transdisciplinary and integrated approach and framework using systems development principles and concepts, and scientific, technological, and management methods.

Standards:

8.1.4.1 Establish, balance and integrate stakeholders' goals, purpose and success criteria, starting in the planning phase and continuing through the entire lifecycle.

8.1.4.2 Establish lifecycle model, process approach and governance structures, considering the levels of complexity, uncertainty, change, and variety.

8.1.4.3 Develop processes and governance models that will enable the development of standard baseline solution architectures across the contract.

8.1.4.4 Develop contract wide processes and governance models that will enable the uniform application and execution of systems engineering, mission assurance, quality assurance, configuration management practices as they are defined in each task order.

8.1.4.5 Perform design synthesis and system verification and validation.

8.1.4.6 Integrate relevant disciplines and groups into a cohesive effort, forming a structured development process that proceeds from concept to production, operation, evolution and eventual disposal.

8.1.4.7 Demonstrate MDIOC facility lifecycle management to ensure the viability of the MDIOC facility from an infrastructure perspective.

8.1.4.8 Demonstrate purchasing economies of scale across the contract in executing procurement strategies and report the efficiencies gained in the Task 8.1 Status Report.

8.1.5 Agile Management

The contractor shall develop and implement agile management and leadership principles. These principles shall prioritize meeting contract requirements while ensuring customer satisfaction, adaptability to change, frequent delivery of workable outputs, collaboration, and continuous improvement. The following table highlights the differences between conventional and agile management

Aspect	Conventional Management	Agile Management
Flexibility	Limited scope for changes; rigid top-down approach.	High adaptability; encourages experimentation and alterations.
Ownership and transparency	Sole ownership by Project Manager; limited team input.	Shared ownership among managers, team members, and customers; collaborative planning.
Problem-solving	Team members need manager's approval for issue resolution; potential delays.	Teams empowered for autonomous problem-solving; swift internal resolutions. Escalation for major decisions.
Checkpoints and progress monitoring	Focus on streamlining processes; minimal guidance; infrequent evaluations.	Regular checkpoints; continuous progress updates; emphasis on iterative feedback.

Standards:

8.1.5.1 Provide robust stakeholder engagement, continuous updates and feedback loops to ensure stakeholder requirements are met throughout the process.
8.1.5.2 Demonstrate capability to swiftly capture emerging and evolving customer requirements. Provide rapid resonses through a change management process that includes Rough Order of Magnitudes (ROMs) and schedule impacts.
8.1.5.3 Continously deliver increment outputs with defined release and sprint cycles to enable more frequent stakeholder feedback and informed adjustments and decisions.

8.1.5.4 Establish and maintain collaboration, communication and alignment between business stakeholders and technical teams.

8.1.5.5 Adopt communication methods that enable continuous and open communication between team members, across Government and contractor teams, including functional organizations and leadership..

8.1.5.6 Measure progress based on the delivery of tangible results/working outputs.

8.1.5.7 Provide continuous improvement and emphasis on requirements delivery while striving for technical excellence and explore measureable innovative approaches, evolve practices, and seek ways to enhance performance.

8.1.5.8 Simplify and optimize work efforts by focusing on essential tasks and streamlining processes.

8.1.5.9 Develop self-organizing and multi-skilled teams with the autonomy and trust to enable informed decisions and independent operations. Empower teams to implement innovative solutions that provide initial capabilities to meet immediate needs that can be matured and modified to support emerging needs.

8.1.5.10 Provide continuous transparency into the Agile Management process through metrics and artifacts that are reported and delivered through an Agile Integrated Management dashboard and in the Task 8.1 Status Report.

8.1.6 Digital Framework

As the MDA is currently developing agency-wide digital governance, this section aims to establish an interim digital framework specific to the MIOES contract. Paragraph 8.1.6 outlines the development of a digital framework independent of broader Agency efforts, to be implemented within the MIOES contract until agency-wide governance becomes more defined. Eventually the agency-wide digital governance will be applied to the MIOES contract, but in the meantime, this framework will guide digital initiatives within the scope of this contract. The intent of this task is for the contractor to develop and adopt digital principles, tools, processes into their operations from the inception of the contract. An example of this is with Task 8.1.3, Program Integration. As the contractor develops the tools, processes, methodologies required to execute Program Integration requirements, the contractor shall develop and adopt digital principles, tools, processes in the execution of these requirements.

The contractor shall build a digitally-empowered contract that establishes a MIOES-specific ecosystem equipped with technology and intuitive processes that facilitate model-based enterprise decision-making, enable automation, institutionalize approved open architectures, and leverage authoritative models and data to ensure seamless stakeholder collaboration, integration, transparency, and engineering rigor across the MIOES contract. This framework shall serve as the foundation for standardizing digital products and deliverables specific to the MIOES contract that will be identified in individual task orders. The contractor shall synchronize activities for efficiency and consistency, apply best practices to add velocity and transparency, and synchronize data in Authoritative Sources of Truth for solution fidelity and work acceleration. These practices shall be implemented with the goal of establishing consistent, replicable processes for digital product development and delivery within the MIOES contract scope.

Standards:

8.1.6.1 Institutionalize the development, integration, and application of models to guide decision-making at both the enterprise and program levels, accelerating capability delivery through streamlined processes, digital-first governance, and the integration of tools, data and processes, while fostering continuous innovation by incorporating models and tools into the concept and design phases to ensure forward-thinking interoperable solutions.

8.1.6.2 Establish and maintain reliable Authoritative Sources of Truth.

8.1.6.3 Develop and sustain digital infrastructure environments that drive activity execution, stakeholder collaboration, and seamless communication.

8.1.6.4 Identify data integration opportunities in the 8.1 status report and then execute as identified.

8.1.6.5 Integrate data into Authoritative Sources of Truth, including Extract, Transform, Load (ETL) processes for data cleaning, format alignment, and centralization to enhance data discoverability and usability.

8.1.6.6 Identify cost efficiencies, improvements in capability, performance, and user experience through continuous feedback to refine solutions and operational practices and document them in the 8.1 Status Report .

8.1.6.7 Identify opportunities for digital practices across the MIOES contract and document them in the 8.1 Status Report.

8.1.6.8 Ensure digital models and data are accompanied by comprehensive descriptions and accessible to all relevant stakeholders from a central location.

8.1.6.9 Report how the standards of this objective have been met in the Task 8.1 Status Report.

8.1.7 Digital Business Strategy

In alignment with the MIOES-specific digital framework outlined in section 8.1.6, the contractor shall incorporate digital technologies and principles in developing and executing business, operational, program integration, and contract data management processes and practices across the MIOES contract. The contractor shall incorporate digital-centric models, adopt digital platforms and architectures, leverage data analytics, and create digital customer experiences. These efforts shall adhere to the standardization guidelines established for MIOES digital products and deliverables. The contractor shall ensure digital processes established under the MIOES contract are centralized and authoritative.

8.1.7.1 Model-Based Decision-Making. The contractor shall develop, integrate, implement, and leverage models to enhance enterprise and program decision-making processes.

Standards:

8.1.7.1.1 Outline and implement a detailed plan for model creation, curation, and seamless integration in the Management Plan

8.1.7.1.2 Apply models directly to work activities, analyses, and decision-making processes

8.1.7.1.3 Provide program integration across the contract through enhanced model utilization

8.1.7.1.4 Report how the standards of this objective have been met in the Task 8.1 Status Report.

8.1.7.2 Digital Communication Transformation. The contractor shall develop digital models and data as the primary communication medium within the MIOES contract.

Standards:

8.1.7.2.1 Establish a robust framework for the management, access, and distribution of information via a unified set of digital models and data.

8.1.7.2.1 Provide continuous access to up-to-date and authoritative information for all stakeholders.

8.1.7.2.2 Report how the standards of this objective have been met in the Task 8.1 Status Report.

8.1.7.3 Technology and Infrastructure for Digital Business. The contractor shall identify and adopt technologies and infrastructure to adopt digital business practices and stakeholder collaboration within the MIOES contract.

Standards:

8.1.7.3.1 Identify and incorporate digital technologies, tools, and processes that bolster business operations

8.1.7.3.2 Determine the necessary infrastructure and environments that facilitate activities, collaboration, and communication both within MIOES and with external stakeholders

8.1.7.3.3 Report how the standards of this objective have been met in the Task 8.1 Status Report

8.1.7.4 Strategic Contract Data Requirements Delivery List (CRDL) Management. The contractor shall manage contract data as a strategic asset, focusing on its collection, protection, accessibility, uniformity, utility, and integrity within the MIOES contract with respect to the data that is required to fulfill the DD Form 1423 collection and reporting requirements and other business functions that require the collection, storage, and reporting of data, e.g. property reporting, cost reporting, integrated scheduling.

Standards:

8.1.7.4.1 Develop and maintain a Master MIOES CDRL Data Catalog associated with this data, including a comprehensive list of Authoritative Data Sources with relevant metadata attributes to ensure data interoperability and sharing (DAL).

8.1.7.4.2 Provide MIOES contract-wide CDRL data access and availability.

8.1.7.4.3 Identify and implement strategies for the elimination of redundant CDRL data and/or CDRL data deliveries and maintain high-quality data standards.

8.1.7.4.4 Incorporate considerations for the digital environment and its implementation in all developed CDRL management processes.

8.1.7.4.5 Identify Government dependencies necessary for the success of Digital Business Transformation initiatives, including Government-furnished information, process changes, or other required Government support.

8.1.7.4.6 Report how the standards of this objective have been met in the Task 8.1 Status Report.

8.1.7.5 Data Utilization. The contractor shall develop and execute solutions that are sustainable within the MIOES contract , avoiding proprietary solutions to ensure continuity and data rights.

Standards:

8.1.7.5.1 Implement best practices for data integration into the Authoritative Source of Truth, including ETL processes for data cleaning, format adjustment, and centralization.

8.1.7.5.2 Facilitate easy data discovery, usage, and translation into actionable business insights.

8.1.7.5.3 Launch educational campaigns to empower end-users and stakeholders on problem-solving with data.

8.1.7.5.4 Develop and maintain a living document that incorporates lessons learned and best practices from both MDA and industry, guiding configuration management and data delivery.

8.1.7.5.5 Report how the standards of this objective have been met in the Task 8.1 Status Report.

8.1.8 Continuous Cost Reduction/Process Optimization/Performance Improvement

The contractor shall implement a continuous Cost Reduction/Process Optimization/ Performance Improvement Program without impairing suitability or quality, or the fit/form function of the product or service that is realistic and can be sustained. The contractor shall instill within the workforce a climate that rewards efforts to continuously improve performance, optimize/streamline processes and reduce costs.

Standards:

8.1.8.1 Document a Continual Improvement plan in the Program Management Plan (PMP) CDRL that flows down applicable industry standards and best practices and centralizes a CI management capability using integrated processes and tools to proactively identify CI opportunities.

8.1.8.2 Develop a cost/process/performance efficiency roadmap in the MIOES Management Plan using applicable industry standards.

8.1.8.3 Develop and implement feedback collection mechanisms for proactive identification of CI opportunities.

8.1.8.4 Identify at least two opportunities for cost control/process optimization/performance improvement every six months and present in the 8.1 Status Report.

8.1.8.5 Develop and submit a CI implementation plan for the chosen opportunity that includes an Organizational Impact Assessment (OIA) or Business Case that documents the analysis of resources required, estimated cost of improvements, operational impacts, schedule, risk matrix, stakeholder feedback and recommendations, and related training requirements.

8.1.8.6 Report actions, results to include the cost savings of the Cost Reduction/Process Optimization/Performance Improvement Program in the Task 8.1 Status Report.

8.1.8.7 Recommend government processes that might require amendments to ensure alignment between government and contractor processes in the Task 8.1 Status Report.

8.1.9 Supply Chain Risk Management

The purpose of Supply Chain Risk Management (SCRM) is to proactively identify supply chain vulnerabilities, threats, and potential disruptions and implement mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found. SCRM is used to avoid disruptions and ensure mission effectiveness and program success.

The contractor shall identify, assess, plan for, report, and mitigate actual or potential threats, vulnerabilities, and disruptions to the contract supply chain throughout its lifecycle to ensure mission effectiveness.

The contractor shall establish, document, and maintain documentation about subcontractors/suppliers/vendors for all parts that will be used for this contract. The contractor shall continuously monitor its sources of supply for unknown, unauthorized, non-certified, or unqualified sources providing parts or services from any sub-tier supplier within the contractor's supply chain.

Standards:

8.1.9.1 Comply with DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).

8.1.9.2 Deliver and implement a Supply Chain Risk Management Plan that identifies the risks to the supply chain and the risk management strategies to be employed to counter those risks, identify critical components and subcomponents in their system design, describe how they will ensure visibility into the supply chain, and ensure the integrity of those critical components and subcomponents. (CDRL A8.1.09)

8.1.9.3 Investigate, resolve, and submit findings consisting of root causes, impacts, and corrective action in accordance with the submitted SCRM Plan.

8.1.9.4 Flow down the requirement to develop and maintain a SCRM Plan to the lowest levels of the supply chain spanning the entirety of the supply chain.

8.1.9.5 Establish, and document processes to verify critical function components received from suppliers are free from malicious code, counterfeit parts, or unauthorized product substitution (e.g., seals, inspection, secure shipping, testing) within and in accordance with DoD 5200.44 and the SCRM Plan.

8.1.9.6 Establish and document processes that address the appropriate controls to ensure subcontractor’s plans comply with SCRM requirements in accordance with DoD 5200.44.

8.1.9.7 Develop and maintain a Supply Chain Risk Register which contains the risk identification information and current status on risks relative to the products and services which the Prime contractor, its suppliers, and subcontractors provide.

8.1.9.8 Communicate actual and potential supply chain risks in accordance with the Risk Register.

8.1.10 Small Business Operations Planning and Reporting

The contractor shall identify potential Small Business (SB) specialty subcontractors and provide regular and transparent feedback on the status of Small Business contract activities.

Standard:

8.1.10.1 Deliver and implement a Small Business Participation Report (Attachment J-XX) to develop capabilities of small businesses, provide maximum practicable opportunity for small businesses to participate in efficient contract performance. (CDRL A8.1.10)

8.1.11 Security and Protection

This contract is a critical element to MDA achieving its mission through a layered defense in depth approach. The contractor shall be responsible for the protection and defense of agency systems that support the defense of our homeland and allied nations.

The contractor shall comply with aspects of security including information, personnel, operational, physical, export control, and cybersecurity in accordance with Federal, DoD, and MDA regulations, policies, procedures, standards, and guidelines.

Standards:

8.1.11.1 Protect MDA-identified Critical Program Information (CPI) and Critical Technologies (CTs) to the standards required in DoD Instruction (DoDI) 5200.39, Critical Program Information (CPI) Identification throughout the lifecycle of the program.

8.1.11.2 Meet and maintain moderate or below compliance requirements of all information systems in accordance with regulations such as Federal Information Security. Modernization Act (FISMA), the NIST Risk Management Framework (RMF), and NIST Special Publications 800 series guidance to protect CUI, PII and classified information.

8.1.11.3 Identify and track the skills and roles required to build and maintain a comprehensive cyber resilient program that incorporates zero trust principles, ensuring systems uphold the highest level DoD and MDA cybersecurity compliance requirements throughout their lifecycle.

8.1.11.4 Integrate cyber into the planning, design, and implementation of all products and services delivered to the MDA in accordance with DoDI 5000.90.

8.1.11.5 Operate, maintain, defend and protect contractor-managed systems and resources IAW cybersecurity requirements throughout the lifecycle.

8.1.11.6 Continuously monitor managed networks and enclaves to identify unauthorized hardware/software products and/or versions.

8.1.11.7 Review Security Classification Guides annually and monitor for possible security violations within Cyber AOR and take action to report incidents under the appropriate task order.

8.1.12 Cybersecurity

All data that is controlled unclassified information (CUI) on nonfederal information systems shall be protected in accordance with National Institute of Standard and Technology (NIST) SP 800-171 (latest revision).

8.1.12.1 Information Management and Control Plan (IMCP)

The contractor shall flow the IMCP to their 1st tier subcontractors with the requirement to flow down the IMCP to all tiers of the supply chain that utilize CUI. Through the IMCP, the contractor shall address implemented practices to minimize and restrict the sharing and/or flow of CUI down the entire supply chain to only those suppliers who have a need-to-know/lawful government purpose. This includes minimizing the information provided on contracts/purchase orders for procurement of logistics and transportation services, systems, or critical components. The contractor shall also address in the IMCP its plan for providing adequate security and for executing cyber incident reporting.

Standards:

8.1.12.1.1 Provide security on covered Contractor information systems in accordance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (hereafter referred to as "DFARS 7012") (if Other Transaction Authority (OTA) or Procurement for Experimental Purposes (PEP) note Article 1, "Safeguarding Controlled Unclassified Information and Cyber Incident Reporting.") Hereafter, Covered Defense Information (CDI), CUI, Technical Data, or Operationally Critical Support information is referred to as CUI.

8.1.12.1.2 Maintain the IMCP throughout the period of performance and deliver periodic updates (CDRL A8.1.10).

8.1.12.1.3 Document suppliers that receive or generate CUI in performance of the contract/agreement in an IMCP Supplier Compliance Supplement (SCS) to the IMCP.

- The SCS Template is located at https://www.mda.mil/global/documents/pdf/IMCP_Supplier_Compliance_Supplement.pdf (This sub-bullet will be placed in the DD1423

8.1.12.1.4 Make available the System Security Plan (SSP) and Plan of Action and Milestones to the COTR as needed.

8.1.12.2 Marking, Delivery, and Destruction

The contractor shall use Department of Defense Instruction (DoDI) 5200.48, "Controlled Unclassified Information," and any applicable Security Classification Guide for the

identification, marking, safeguarding, dissemination, records management, and destruction of CUI.

Standards:

8.1.12.2.1 Adhere to Department of Defense Instruction (DoDI) 5200.48, “Controlled Unclassified Information.

8.1.12.2.2 Adhere to Information Security Oversight Office Notice 2019-03, “Destroying Controlled Unclassified Information in Paper Form.”

8.1.13 Continuity of Services

The contractor shall develop and execute a MIOES contract phase-out plan that provides for an orderly and effective transition of products and services to the follow-on contractor(s) with no interruption or impact to mission.

Standards:

8.1.13.1 Deliver a Program Phase-Out Plan to establish plans for the transition activities that may occur during the last six months of the period of performance. (CDRL A8.1.12)

8.1.13.2 Include TO transition and close-out plans, information exchange with in the incoming contractor, and a shadowing plan that will give incoming contractor personnel insight into the projects and events that will continue through the contract transition.

8.1.13.3 Include routine tag-ups between the MIOES contractor, the follow-on contractor, and MDA representatives to discuss status, schedules, and identify and resolve issues.

8.1.13.4 Capture issues and lessons learned during the MIOES Phase-In process to inform and shape the Program Phase-Out Plan to ensure products and services are transitioned from MIOES to the follow-on contractor(s) with no interruption or impact to mission.

8.1.13.5 Cooperate fully to permit an effective, orderly, and successful transition from MIOES to the follow-on contract(s).

8.1.13.6 Include TO continuity logs that minimize learning curves for the follow-on contractor(s).

8.1.13.7 Establish modular, digital, processes and information systems that will allow straightforward data transfer for ongoing projects and events to ensure the legacy of projects that extend over performance periods is retained.

8.1.14 Mission Engineering

The DoD Mission Engineering Guide states; “Mission engineering is a process that helps the DoD better understand and assess impacts to mission outcomes based on changes to systems, threats, operational concepts, environments, and mission architectures.” The following Mission Engineering activities shall be performed at the task order level.

8.1.14.1 Systems Engineering

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Systems Engineering Program.

Standards:

8.1.14.1.1 Operate within standardized systems engineering (SE) principles, processes, and operations across the task order.

- Create and apply consistent engineering standards.
- Track, assign, and align requirements in accordance with requirements baseline standards.
- Define products and services with architectures and assigned technical ownership in accordance with architectural baseline standards.
- Track assets in accordance with engineering baseline standards.

8.1.14.1.2 Align with contract level systems engineering governance, based on the MDA/MDIOC Systems Engineering Plans and MIOES Systems Engineering Management Plan, and demonstrate adherence to and participation in contract level systems engineering activities.

8.1.14.1.3 Implement standardized Digital Engineering/Model-Based Systems Engineering (DE/MBSE) principles that are in alignment with MDA DE/MBSE initiatives, shifting the focus from traditional methods and document-based deliverables and artifacts to a model-centric perspective, where SE activities are performed by leveraging digital artifacts and models.

8.1.14.1.4 Provide standardized development and maintenance of the technical baseline standards and that they address each of the component baselines:

- Requirements Baseline
- Architectural Baseline
- Engineering Baseline

8.1.14.1.5 Demonstrate SE knowledge and excellence practices to enable a common awareness of project status and delivery of real-time and accurate data.

8.1.14.1.6 Implement consistent SE processes to ensure repeatable performance across the task order.

Participate in the MDIOC Engineering Review Board IAW the MDIOC SEP and ERB governance.

8.1.14.1.7 Capture and provide requirements, architectural, and engineering components required for the MDIOC Facility Systems Technical Baseline in accordance with the MDIOC Technical Baseline Standard. Maintain contributing artifacts in configuration managed authoritative data sources.

8.1.14.1.8 Comply with hardware and software engineering standards.

8.1.14.1.9 Report on the health and status of this task order's compliance with the MIOES SE program in the 8.1 Status Report.

8.1.14.2 Mission Assurance

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Mission Assurance Management Program.

Standards:

8.1.14.2.1 Operate within standardized MA principles, processes, and operations across the task order. Provide mission assurance for concurrent operations of systems and services, to include event and resource de-confliction and mission/event asset protection.

8.1.14.2.2 Provide task order level activity and project updates to the MDIOC Range Integrated Schedule (MRIS) production team as necessary. Ensure Event Protection Period (EPP) schedules that are applicable to this task order are shown on the MRIS, as well as other available test and project schedules, and all other pertinent information.

8.1.14.2.3 Report MDIOC-impacting, real world, and event MA information applicable to this task order to a common location (e.g., MA dashboard) to enable shared and reliable situational awareness across the enterprise.

8.1.14.2.4 Provide incident reporting IAW the MDIOC Incident Notification Procedure.

8.1.14.2.6 Participate in Work Screening Team (WST) activities during EPPs to review and authorize physical work taking place at the MDIOC to prevent mission and event impacts from occurring.

8.1.14.2.7 Refrain from performing physical work at the MDIOC during EPPs without WST approval.

8.1.14.2.8 Submit changes to the MDIOC DML as required.

8.1.14.2.9 Report on the health and status of this task order's compliance with the MIOES MA program in the 8.1 Status Report.

8.1.14.3 Mission Assurace (Risk Management)

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Risk Management Program.

Standards:

8.1.14.3.1 Operate within standardized risk management (RM) principles, processes, and operations across the task order.

8.1.14.3.2 Perform horizontal integration of task order risk management for task order level systems/events across the MIOES contract.

8.1.14.3.3 Perform vertical risk management integration across all areas of risk, including technical, cost, schedule, safety, supply chain, and security within the task order and its suppliers, and address any gaps.

8.1.14.3.4 Report on the health and status of this task order's compliance with the MIOES RM program in the 8.1 Status Report.

8.1.14.4 Configuration Management

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Configuration Management Program.

Standards:

8.1.14.4.1 Operate within standardized configuration management (CM) principles, processes, and operations across the task order.

8.1.14.4.2 Place MDIOC Facility systems Technical Baseline artifacts related to changes approved by the MDIOC ERB into an authoritative data repository, to include controlling who can view, edit or update artifacts IAW MDIOC change procedures.

8.1.14.4.3 Document and classify engineering change requests as Class I or II for consideration by the appropriate change authority.

8.1.14.4.4 Obtain approval by the appropriate MDIOC/MDA board, per MDA Manual 3500.1-M, Class I changes that affect the form, fit, or function of a baseline configuration and have the potential to increase risk, decrease performance, or impact a mission-critical system.

8.1.14.4.5 Obtain approval by a MIOES configuration control board for Class II changes that do not meet the requirements for government involvement.

8.1.14.4.6 Participate in the MIOES Configuration Control Board.

8.1.14.4.7 Report on the health and status of this task order's compliance with the MIOES CM program in the 8.1 Status Report.

8.1.14.5 Quality Management

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Quality Management Program.

Standards:

8.1.14.5.1 Operate within standardized quality management (QM) principles, processes, and operations across the task order and provide consistent implementation of codes, standards, and procedures.

8.1.14.5.2 Demonstrate AS9100-compliant core processes and quality management adherence to MIOES level quality management activities.

8.1.14.5.3 Develop, manage, coordinate, track and report Corrective Actions and Lessons Learned efforts to resolve identified deficiencies and prevent reoccurrence.

8.1.14.5.4 Participate in and support the audit program.

8.1.14.5.5 Report on the health and status of this task order's compliance with the MIOES QM Program in the 8.1 Status Report.

8.1.14.6 Enterprise Architecture

The contractor shall participate in and ensure all task order activities are in compliance with and align to the MIOES Enterprise Architecture (EA) Program.

Standards:

8.1.14.6.1 Operate within standardized enterprise architecture (EA) principles, processes, and operations across the task order.

8.1.14.6.2 Implement a common Enterprise Architecture vision across the task order to support MDA "to-be" architectures, including the identification of gaps and lessons learned.

8.1.14.6.3 Establish technical baseline repository standards across the task order for historical artifacts, the provenance of those artifacts, and supporting data to include deliverables and artifacts created for and shared with MDA stakeholders.

8.1.14.6.4 Report on the health and status of this task order's compliance with the MIOES EA Program in the 8.1 Status Report.

Attachment 2

Task 8.2

Background: Task 8.2 will be placed in each MIOES task order. This represents the top-level task order management and leadership requirements. These requirements will be tailored in each task order.

8.2 Task Order Management

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 MDA CWQT.

8.2.1.11 Develop and deliver a Cybersecurity Resiliency Management Plan (CDRL) (This standard will only reside in the Enterprise IT Services task order):

- Initial assessment within 6 months of contract award.
- Full plan with milestones delivered within 1 year of award.
- Update annually or as security-relevant changes occur.

8.2.1.12 Lead, manage, and execute TO activities in accordance with the approved Cyber Resiliency Management Plan.

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

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) (CDRL A002)

- One of three IPMDAR CDRLs will be incorporated, based on contract type and TO dollar value

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.

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

8.2.2.6 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 A003)

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 ensure a seamless closeout of TO activities.

Standard:

8.2.4.1 Perform a TO closeout that consolidates all TO data and deliver a Task Order Close-Out Report. (CDRL A004)

Attachment 3

DoD Issuances

The following issuances are applicable to all task orders issued under the contract. Tailoring, as necessary, may be done at the task order level.

The MIOES contractor shall comply with all directives listed. If a referenced directive requires compliance with one or more secondary directives, those secondary directives are to be consider guidance in the execution of the PWS requirements unless specifically included in the task order PWS or this attachment. When directive chapters, paragraphs, appendices, attachments, etc. are referenced as a standard in a Task Order, the standard shall be inclusive of all subordinate paragraphs unless specifically excluded. For example, if the standard lists paragraph 1.2 and paragraph 1.2 has subparagraphs 1.2.1, 1.2.1.1 and 1.2.1.2, those subparagraphs are directive.

The contractor shall stay up to date on all directive updates. Contractor execution shall comply with the current version of the directives. The contractor shall notify the Contracting Officer in writing within 30 days of directive revision, change, supplement, and/or rescission. If there is any cost impact resulting from such revisions, changes, supplements and rescissions the contractor shall provide the cost information with the notification; increases or decreases in the negotiated task order cost / price will not become effective until directed by the Contracting Officer. If the Contracting Officer is not notified in writing within 30 days, the contractor shall perform in accordance with directive revisions, changes, supplements and rescissions at no increase to the negotiated task order cost / price. The Contracting Officer retains the right to negotiate downward revisions to the negotiated task order cost / price should the Government become aware of decreases in requirements as a result of modifications to directives.

DoD Directives

1. DoDD 8000.01, Management of the Department of Defense Information Enterprise (DoD IE), 17 Mar 2016 with Change 1, 27 Jul 2017
2. DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 Apr 2004, Certified Current as of 23 Apr 2007
3. DoD Directive 8140.01, “Cyberspace Workforce Management,” 5 October 2020

DoD Instructions

4. DoDI 4140.01, DoD Supply Chain Material Management Policy, 6 Mar 2019
5. DoDI 5200.48, Controlled Unclassified Information, 6 Mar 2020
6. DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security (CS) Activities, 29 Jan 2010 with Change 2, 21 Aug 2019
7. DoDI 5400.11, DoD Privacy And Civil Liberties Programs, 29 Jan 2019 with Change 1, December 8, 2020

8. DoDI 6055.1, DoD Safety and Occupational Health (SOH) Program, 14 Oct 2014 with Change 3, Apr 21, 2021
9. DoDI 8310.01, Information Technology Standards in the DoD, 7 Apr 2023
10. DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 3 Nov 2017
11. DoDI 8500.01, Cybersecurity, 14 Mar 2014 with Change 1, 7 Oct 2019
12. DoDI 8510.01, Risk Management Framework for DoD Systems, 19 Jul 2022
13. DoDI 8520.02, Public Key Infrastructure And Public Key Enabling, 18 May 2023
14. DoDI 8540.01, Cross Domain (CD) Policy, 8 May 2015 with Change 1, 28 Aug 2017
15. DoDI 8551.01, Ports, Protocols and Services Management, 31 May 2023
16. DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 Jul 2004
17. DoDI 8582.01, Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information, 9 Dec 2019

DoD Manuals

18. DoDM 5000.04, Cost And Software Data Reporting, 7 May 2021
19. DoDM 8140.03, Cyber Workforce Qualification and Management Program, 15 Feb 2023)
20. DoDM 8180.01, Information Technology Planning for Electronic Records Management, 4 Aug 2023
21. DoDM 8530.01, Cybersecurity Activities Support Procedures, 31 May 2023

MDA Directives

22. MDA 3200.06, Missile Defense Test Data/Information Management, 13 Jan 2022
23. MDA 5000.15, Missile Defense System Requirements Traceability Process, 22 Feb 2024
24. MDA 5200.01, Security Policy, 23 Aug 2023
25. MDA 5230.02, International Security, 23 Aug 2021
26. MDA 6055.01, Occupational Safety and Health Program Management, 6 Apr 2020
27. MDA 8180.01, Enterprise Records Management, 15 Mar 2021

MDA Instructions

28. MDA 1400.07-INS, In-and-Out Processing Procedure, 14 Sep 2016 (Under Revision in TMT. 9/14/2023 Cancellation date listed)
29. MDA 3000.02-INS, Missile Defense System Asset Management, 28 Sep 2023
30. MDA 3058.01-INS, Risk Management, 18 Feb 2016.
31. MDA 3200.07-INS, Flight Test Viewing and Notification, 2 Apr 2021
32. MDA 3500.01-INS, Missile Defense System Change Management Process, March 11, 2021
33. MDA 5004.01-INS, Missile Defense System Integrated Baseline Reviews, 25 Jan 2021

34. MDA 5200.02-INS, Information Security Program, 22 Mar 2018

35. MDA 5205.02-INS, Missile Defense Agency Operations Security Program, 24 May 2023

36. MDA 5230.01-INS, Foreign National Visits, Assignments, and Event Participation at the Missile Defense Agency, 1 Aug 2022

37. MDA 6055.02-INS, Accident Investigations and Reporting, 19 Nov 2018

38. MDA 6055.04-INS, Work Time Restrictions for Safety and Mission Critical Personnel Supporting Tests and Critical Operations, 11 Sep 2023

39. MDA 8110.01-INS, Privacy Civil Liberties Program, 12 Oct 2022

40. MDA 8400.01-INS, Sustainable Electronics Management Program, 13 Oct 2020

MDA Manuals

41. MDA 5003.01-M, Missile Defense System Earned Value Management, 21 July 2021

42. MDA 5004.01-M, Missile Defense System Integrated Baseline Reviews, 1 Feb 2021

43. MDA 5200.08-M, Procedures for Protection of Critical Program Information, Mission Critical Functions, and Critical Components Within the Missile Defense Agency, 1 May 2019

Miscellaneous

44. MDA Policy Memorandum No. 12, Missile Defense Agency Director's Safety Policy, 13 Nov 2023

45. MDA-QS-001, Missile Defense Agency Assurance Provisions (MAP) Rev C, 1 Oct 2019

46. MDA Information Management Processes and Information Technology Operations, MDA, 28 May 2003

47. MDA Information Technology Continuity Of Operations and Disaster Recovery Plan v4.0, MDA/ICT, Oct 2015.

48. MDA IT Mission Support Facilities Design Guide, MDA/ICT, 3 Feb 2009

49. MDA User Accounts and Password Management Guidance, MDA/ICT, 24 Aug 2007

50. MDA CIO Use and Control of Wireless Mobile Devices (Government Issued and Personally Owned) in MDA Facilities, MDA/ICT, 8 Oct 2013 (Recommend 8100.02-INS, Wireless Mobile Devices, 7 Aug 2017 with Change 1, 30 Nov 2017. Under Revision in TMT. This instruction establishes standard policy and procedures for the use and control of wireless mobile devices by all personnel working for the Missile Defense Agency (MDA) and for visitors to MDA-controlled facilities)

51. DA-1510-014-840266 MDA Core Services Directory Services Naming Conventions, MDA/ICT, 21 Jun 2018

52. Executive Order 13834, Federal Leadership in Environmental, Energy, and Economic Performance, Section 6 (Duties of the Federal Chief Sustainability Officer, Section 7 (Duties of Heads of Agencies), and Section 11 (General Provisions); Executive Order 13990 Climate Crisis; Efforts to Protect Public Health and Environmental and Restore Science, 25 Jan 2021 (Recommend 8400.01-INS, Sustainable Electronics Management

Program, 15 Feb 2022. Program to establish sustainable electronics management policies. These policies are designed to increase electronics life usage, save money through reduced energy consumption, reduce associated greenhouse gas emissions, divert landfill waste, reduce waste toxicity, and disposals.)

53. DoD Memorandum, Software Development and Open Source Software , 24 Jan 2022

54. CJCSI 6211.02D, Defense Information System Network (DISN) Responsibilities, 24 Jan 2012, Current as of 4 Aug 2015

55. CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 Feb 2011, Current as of 9 Jun 2015

56. CJCSI 6510.06C, Communications Security Releases to Foreign Nations, 3 Apr 2019

57. Strategic Command Directive (SD) 527-1, Department of Defense (DoD) Information Operation Condition (INFOCON) System Procedures, 27 Jan 2006

58. DAFI 32-2001, Fire and Emergency Services (F&ES) Program, 28 July 2022

59. AFMAN 32-7002, Environmental Compliance and Pollution Prevention, 4 Feb 2022

60. DAFI 63-101/20-101, Integrated Life Cycle Management, 16 Feb 2024

61. AFI 90-821, Hazard Communication (HAZCOM) Program, 13 May 2019

62. AFI 32-1024, Standard Facility Requirements, 14 Jul 2011

63. 50th Space Wing Host Tenant Support Agreement, FB2502-14118-0500, 3 Jul 2018

64. National Policy Governing the Acquisition Of Information Assurance (IA) and IA-Enabled Information Technology Products (CNSS Policy No. 11) 10 June 2013

65. CFR, Title 29, Subtitle B, Chapter XVII, Occupational Safety and Health Administration, parts 1910 (Occupational Safety and Health Standards), 1926 (Safety and Health Regulations for Construction), and 1960 (Basic Program Elements for Federal Employee Occupational SAFETY and Health Programs and Related Matters), Up to date as of 4 Apr 2024

66. MIL-STD-882E, Department of Defense Standard Practice: System Safety, 11 May 2012 with Change 1 27 Sep 2023

67. MIL-STD-46855A, Human Engineering, Processes Requirements for Military Systems, Equipment, and Facilities, 24 May 2011, Notice 2, 21 Dec 2020

68. MIL-HDBK-61B, Department of Defense Handbook: Configuration Management Guidance, 7 Apr 2020

69. National Security Telecommunications and Information Systems Security Advisory Information Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance, Appendix K, 30 December 2000. Note for reference: Appendix K of NACSIM 5203 will remain in effect until NACSI 4009, Protected Distribution Systems, dated 30 December 1981, is superseded. NACSI 4009 is currently under revision.

70. Configuration Management Standard EIA649C, May 1998, Revised 7 Feb 2019

71. National Fire Protection Association (NFPA) 70E, Standards for Electrical Safety in the Workplace, 2024
72. International Plumbing Code (IPC), 2021 (New version Jun 2024)
73. International Building Code (IBC), Aug 2023
74. National Electrical Code (NEC), 2023
75. Intelligence Community Directive (ICD) 704, Personnel Security, 1 Oct 2008, Amended 20 Jun 2018
76. Unified Facilities Criteria (UFC) 4-010-01, DoD Minimum Antiterrorism Standards for Buildings, 12 December 2018, Change 2, 30 July 2022
77. Department of Defense (DoD) Enterprise Service Management Framework (DESMF), Edition III, 22 Jun 2016
78. Department of Defense Information Enterprise Architecture (DoD IEA), Version 2.0, Volume I – Management Overview of the DoD IEA, Jul 2012
79. Department of Defense Information Enterprise Architecture (DoD IEA), Version 2.0, Volume II – IEA Description, Jul 2012
80. Federal Enterprise Architecture Framework, Version 2, 29 Jan 2013
81. Missile Defense Agency Systems Engineering Plan (SEP), Revision 4.0, August 31, 2023
82. MDIOC Facility Mission Assurance Plan
83. MDIOC Facility Mishap Prevention and Safety Plan
84. MDIOC Facility Environmental Program Plan
85. MDIOC Facility Evacuation Plan
86. MDIOC Facility Mission Assurance Handbook
87. MDIOC Facility Systems Engineering Plan
88. MDIOC Facility Configuration Management Plan
89. MDIOC Facility Quality Assurance Plan
90. MDIOC Engineering Review Board Charter
91. MDIOC Unified Facilities Guide Specification
92. Intelligence Community Directive (ICD) 705, Sensitive Compartmented Information Facilities
93. Executive Order (EO) 12333, United States Intelligence Activities (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008))
94. CFR Title 44, Emergency Management and Assistance, 9 Sep 2024

95. Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, 28 Jul 2016

96. United States Code (USC), 2018 Edition, Title 40. Public Buildings, Property, and Works, § 11331, Responsibilities for Federal information systems standards, 14 Jan 2019 (CITE AS: 40 USC 11331)

97. USC Title 44. Public Printing and Documents, § 3551, Purposes, Information Security (CITE AS: 44 USC 3551)

98. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, Feb 2004

99. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, 1 Mar 2006

100. Federal Information Security Modernization Act of 2014 (FISMA 2014), 18 Dec 2014

101. CNSSI 1253, Security Categorization and Control Selection for National Security Systems, 27 Mar 2014

102. Committee on National Security Systems Advisory Memorandum (CNSSAM) TEMPEST/01-13, RED/BLACK Installation Guidance, 17 Jan 2014

103. Chairman of the Joint Chief of Staff Manual (CJCSM) 6510.01B, Cyber Incident Handling Program, 18 Dec 2014

104. USC Title 10. Armed Forces, §4324, Life Cycle Management and Product Support, 2021

105. DISA Instruction 270-50-9, Life Cycle Sustainment Planning 3 Feb 2023

106. 22 Code of Federal Regulations [CFR] 120-130 eCFR: 22 CFR Chapter I Subchapter M -- International Traffic in Arms Regulations

107. JFHQ-DODIN OPORD 8600

108. JFHQ-DODIN TASKORD 20-0020

109. DoD Secure Cyber Resilient Engineering (SCRE) System Assurance Guidance, February 2024

110. Information Technology Infrastructure Installation Guide, IC 8350.01, July 8, 2022

National Institute of Standards and Technology (NIST) Special Publications (SP) Library 800 series <https://csrc.nist.gov/publications/sp>

1. NIST SP 800-61 Rev 2, Computer Security Incident Handling Guide, 6 Aug 2012

2. NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, 10 Oct 2019

3. NIST SP 800-34 Rev 1, Contingency Planning Guide for Federal Information Systems, 11 Nov 2010

4. NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations, 10 Dec 2020

5. NIST SP 800-53A Rev 5, Assessing Security and Privacy Controls in Information Systems and Organizations, 25 Jan 2022

6. NIST SP 800-37 Rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 20 Dec 2018

7. NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, 20 Sep 2011

8. NIST SP 800-137A, Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment, 21 May 2020

9. NIST SP 800-60 Vol 1, Guide for Mapping Types of Information and Information Systems to Security Categories (Vol 2: Appendices), 1 Aug 2008

10. NIST SP 800-88 Rev 1, Guidelines for Media Sanitization, 17 Dec 2014

11. NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, 10 Oct 2019

12. NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, 24 Feb 2006

13. NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management, June 2017

Attachment 4
Anticipated Data Item Description/DD Form 1423 Requirements

DID ID#	DID Title	DD Form 1423 Subtitle
DI-FNCL-81765C	Contractor Business Data Report	CCDR DD Form 1921-3
DI-FNCL-82162	Cost and Hour Report (Flexfile)	Contractor Cost Data Reporting (CCDR)
DI-MGMT-82164	Quantity Data Report	Flexfile Contractor Cost Data Report (CCDR)
DI-IPSC-82252A	Vulnerability Assessment Report	
DI-MGMT-80004	Management Plan	
DI-MGMT-82383	Information Management And Control Plan	
DI-MGMT-80368A	Status Report	
DI-MGMT-80441D	Government Property Inventory Report	
DI-MGMT-81334D	Contract Work Breakdown Structure (CWBS)	
BaDI-MGMT-81453A	Data Accession List (DAL)	
DI-MGMT-81468	Contract Funds Status Report	
DI-MGMT-81808	Contractor's Risk Management Plan	
DI-MGMT-81861C	Integrated Program Management Data And Analysis Report (IPMDAR) Full	
DI-MGMT-82256	Supply Chain Risk Management (Scrm) Plan	
DI-MISC-81489A	Real Property Facilities As-Built Drawings	
DI-QCIC-81794	Quality Assurance Program Plan	
DI-SAFT-81563/T	Accident / Incident Report	
DI-SESS-80255A/T	Failure Summary And Analysis Report	
DI-SESS-81315B	Failure Analysis And Corrective Action Report (FACAR)	
DI-MGMT-81580	Contractor’s Standard Operating Procedures	
DI-MISC-81489A	Real Property Facilities As-Built Drawings	
DI-QCIC-81794	Quality Assurance Program Plan	
DI-MGMT-82041B	Small Business Utilization Report	
DI-MISC-80508B	Technical Report–Study/Services	Maintenance and Spare Report
DI-MISC-80508B	Technical Report–Study/Services	Detailed Facility Project Design
DI-MISC-80508B	Technical Report–Study/Services	Asset Management Plan
DI-MISC-80508B	Technical Report - Study/Services	Work Request History
DI-MISC-80508B	Technical Report - Study/Services	Asset Management and Maintenance Report
DI-MISC-80508B	Technical Report–Study/Services	MDIOC Unified Facilities Guide Specification (MUFGS)
DI-MISC-80508B	Technical Report–Study/Services	Preliminary Facility Project Design

DI-MISC-80508B	Technical Report - Study/Services	Technology Refresh Plan
DI-MISC-80508B	Technical Report - Study/Services	MDA/SS Space Planning Layout Documentation
DI-MISC-80508B	Technical Report–Study/Services	Engineering Document, Closeout
DI-MISC-80508B	Technical Report–Study/Services	Facility Project Closeout
DI-MISC-80508B	Technical Report–Study/Services	Engineering Documentation
DI-MISC-80508B	Technical Report - Study/Services	Tenant Cost Report
DI-MISC-80508B	Technical Report - Study/Services	Future Studies
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Fire Suppression and Detection System Description
DI-MISC-80508B	Technical Report - Study/Services	Physical Inventory Reports
DI-MISC-80508B	Technical Report–Study/Services	Assessment and Authorization Documentation
DI-MISC-80508B	Technical Report - Study/Services	Facility Configuration Report
DI-MISC-80508B	Technical Report - Study/Services	Defense Property Accountability System (DPAS) Reconciliation Report
DI-MISC-80508B	Technical Report - Study/Services	Chemical Inventory and Hazardous Material Usage Report
DI-MISC-80508B	Technical Report - Study/Services	Operational Support Documents : MDA Enterprise Strategic Plan
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Electrical Power Distribution System Description
DI-MISC-80508B	Technical Report - Study/Services	Operational Support Documents : MDA CIO Service Portfolio
DI-MISC-80508B	Technical Report–Study/Services	MDIOC Facility Project Implementation Plan
DI-MISC-80508B	Technical Report - Study/Services	Baseline Engineering Documentation
DI-MISC-80508B	Technical Report - Study/Services	Failure Mode, Effects, and Critical Analysis (FMECA)
DI-MISC-80508B	Technical Report - Study/Services	Operational Support Documents: Capacity Management Plan
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Plumbing System Description
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Facility Conditions Assessments (FCAs)
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Roof System Description
DI-MISC-80508B	Technical Report–Study/Services	Test Case Description Document (TCDD)
DI-MISC-80508B	Technical Report - Study/Services	Cyber Incident Handling Process : [FY]
DI-MISC-80508B	Technical Report - Study/Services	MDIOC Facility and System Drawings, Schedules, and Data
DI-MISC-80508B	Technical Report–Study/Services	As-Run Test Procedures (TPs)
DI-MISC-80508B	Technical Report - Study/Services	Cyber Incident Handling Process : [FY]
DI-MISC-80508B	Technical Report - Study/Services	Reference Architecture Reporting
DI-MISC-80508B	Technical Report - Study / Services	MIOES Cybersecurity Risk Management Plan
DI-MISC-80508B	Technical Report - Study/Services	Application Engineering Documentation
DI-MISC-80508B	Technical Report - Study / Services	Cybersecurity Controls Statement of Compliance
DI-MISC-80508B	Technical Report - Study / Services	Cyber Incident or Compromise Report
DI-MISC-80508B	Technical Report - Study/Services	Operational Support Documents : Data Management Plan
DI-MISC-80508B	Technical Report - Study / Services	MIOES Cybersecurity Workforce Management Report
DI-MISC-80508B	Technical Report - Study/Services	Operational Support Documents : CIO Roadmap

DI-MISC-80508B	Technical Report - Study / Services	MIOES Environmental Program Plan
DI-MISC-80508B	Technical Report - Study / Services	MIOES Mishap Prevention and Safety Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Evaluation Plan
DI-MISC-80508B	Technical Report - Study / Services	Task Order Close-Out Report
DI-MISC-80508B	Technical Report - Study / Services	IRES Program Information Management System Documentation
DI-MISC-80508B	Technical Report - Study / Services	Program Phase-Out Plan
DI-MISC-80508B	Technical Report - Study/Services	Software Accountability Report
DI-MISC-80508B	Technical Report - Study / Services	Configuration Management Maturity Assessment
DI-MISC-80508B	Technical Report - Study / Services	Mission Assurance Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Mishap Prevention and Safety Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Environmental Program Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Evacuation Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Mission Assurance Handbook
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Mission Assurance Plan
DI-MISC-80508B	Technical Report - Study / Services	Incident Notification Report
DI-MISC-80508B	Technical Report - Study / Services	MDIOC Facility Quality Assurance Plan
DI-MISC-80508B	Technical Report - Study / Services	MDIOC System Description Document
DI-MISC-80508B	Technical Report - Study / Services	Board Support and Configuration Management Reporting
DI-MISC-80508B	Technical Report - Study / Services	MDSEA Operations Procedures for SKA
DI-MISC-80508B	Technical Report - Study / Services	Chargeback/Showback Metrics Report
DI-MISC-80508B	Technical Report - Study / Services	MDSEA Operations Procedures for MEGS
DI-MISC-80508B	Technical Report - Study / Services	Satellite Operations Status Report
DI-MISC-80508B	Technical Report - Study / Services	System Engineering and Integration
DI-MISC-80508B	Technical Report - Study / Services	Satellite Crew Certifications Completed
DI-MISC-80508B	Technical Report - Study / Services	Ground Segment Procedures Completed
DI-MISC-80508B	Technical Report - Study / Services	Program Protection Implementation Plan (PPIP)
DI-MISC-80508B	Technical Report - Study / Services	MDSOC Crew Certifications Completed
DI-MISC-80508B	Technical Report - Study / Services	SKA Event Support & Planning
DI-MISC-80508B	Technical Report - Study / Services	MDSOC SKA Operations Support Status Reporting
DI-MISC-80508B	Technical Report - Study / Services	MDSOC HBTSS Operations Support Status Reporting

1558
1559
1560

Attachment 5

Cost and Software Data Reporting Plan

Reference Attachment 1

PWS Paragraph 8.1.2, Measurement & Control

CSDR Plan.xls