TECHNICAL, ENGINEERING, ADVISORY and MANAGEMENT SUPPORT (TEAMS)

Performance Work Statement (PWS) for
Information Technology Management and Analysis
(ITMA)
April 27, 2018

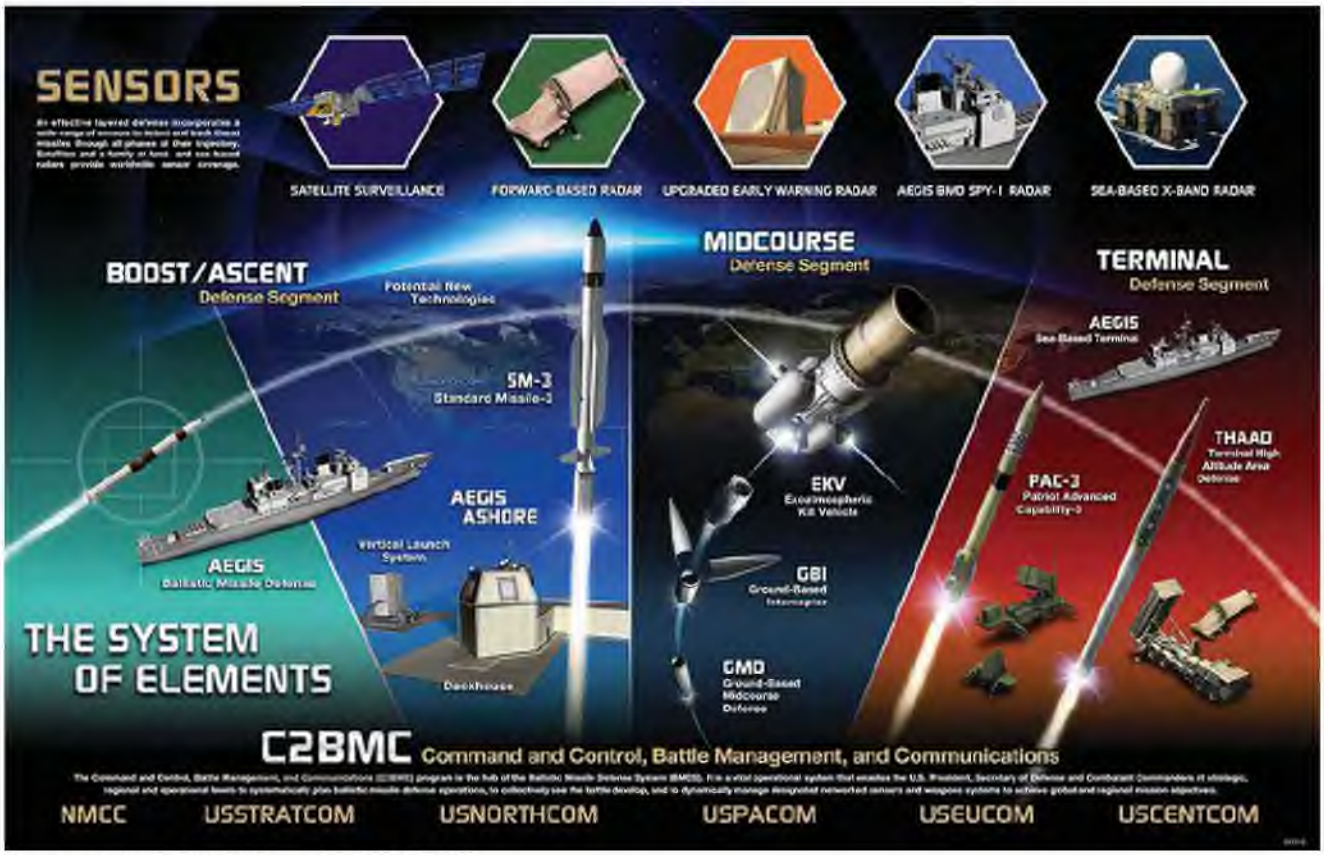
Revision History

Author	Date	MR Number	Reason For Change(s)	PWS Version
(b)(6)	08 Nov 18	1257	Inclusion of Foreign military sales verbiage; Inclusion of increase in Support for Aegis Ashore (AB-FMS) Para 3.3.3.c;	1

1. Top Level Functional Requirements/Scope

1.1. Purpose

The Missile Defense Agency's (MDA) mission is to develop, test, and field an integrated, layered, ballistic missile defense system (BMDS) to defend the United States, its deployed forces, allies, and friends against all ranges of enemy ballistic missiles in all phases of flight. The MDA Chief Information Officer (CIO), a Senior Executive Service (SES) appointment compliant with Clinger-Cohen Act (Pub. L. 104-106), is responsible for providing MDA with Enterprise (Agency-wide) Information Technology (IT) capabilities for Administrative and General Services (GENSER) capabilities servicing the MDA administrative and business requirements as well as general services for BMDS Research, Development, Test, and Evaluation (RDT&E) requirements; plus the cybersecurity lead for the BMDS fielded capabilities and MDA Enterprise. The MDA CIO appoints the MDA Information Systems Authorizing Official (AO) for all of MDA to include the BMDS fielded capabilities.



Approved for Public Release 16-MDA-8540

Figure 1.1: The Ballistic Missile Defense System

Missile defense technology being developed, tested and deployed by the United States is designed to counter ballistic missiles of all ranges—short, medium, intermediate and long. Since

ballistic missiles have different ranges, speeds, size and performance characteristics, the BMDS is an integrated, "layered" architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets.

Ballistic missile trajectories are commonly divided into three phases of flight: boost, midcourse, and terminal. Each element will play an important role in a robust system intended to defend against hostile missiles in any phase of flight.

The BMDS system's architecture includes:

- Networked sensors (including space-based) and ground- and sea-based radars for target detection and tracking;
- Ground- and sea-based interceptor missiles for destroying a ballistic missile using either the force of a direct collision, called "hit-to-kill" technology, or an explosive blast fragmentation warhead; and
- A command, control, battle management, and communications network providing the operational commanders with the needed links between the sensors and interceptor missiles.

The BMDS elements are:

- Aegis Ballistic Missile Defense (BMD)
- Command, Control, Battle Management and Communications (C2BMC)
- Ground-based Midcourse Defense (GMD)
- Sensors
- Terminal High Altitude Area Defense (THAAD)

Each BMDS element has multiple unique components, such as: interceptors, fire control, unique sensors, element internal and external communications capabilities, unique command and control configurations, etc.

1.2 Background

The BMDS weapon system, as depicted in Figure 1.1, is made up of several elements and components. MDA is identified as a rapid acquisition agency with the mission to expedite BMDS capabilities development and testing. MDA then fields demonstrated BMDS program capabilities as soon as they are available.

Information is a strategic asset to MDA, and as such shall be appropriately secured, shared, and made available to the maximum extent possible throughout the information life cycle to MDA workforce.

The MDA CIO office provides MDA with enterprise services, defined as: a common set of information resource capabilities designed to provide awareness of, access to, and delivery of information. Information is defined as: any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic,

cartographic, narrative, or audiovisual forms. This advisory and assistance services requirement will ensure the Office of the CIO is able to:

- Improve information solutions with reliable, timely, accurate information that is protected, secure, and resilient against information warfare, terrorism, criminal activities, natural disasters, and accidents.
- Improve IT investment portfolio alignment with the required DoD Information Enterprise policies and guidance
- Improve operational effectiveness and efficiency through superior IT services delivery
- Improve resilient communications and computing infrastructure
- Improve organizationally-tiered reviews, oversight, and execution to ensure IT investments are in compliance with architectures at various levels, IT standards, and related policy requirements

The MDA CIO office provides administrative net-centric enterprise services to all of MDA through a robust, globally-interconnected network environment (including infrastructure, systems, processes, and people) in which data are shared quickly and seamlessly among users, applications, and platforms. MDA uses mostly DoD available shared administrative (DoD business mission area) tools, such as the Defense Agencies Initiative (DAI) electronic-business suite for government time cards, or the Defense Travel System (DTS) for government travel arrangements, or the DoD Civilian Acquisition Workforce Personnel Demonstration Project's (AcqDemo) Contribution-based Compensation and Appraisal System (CCAS) CAS2Net system for government civilian appraisal processes. The MDA unique administrative services are all based on commercial-off-the-shelf (COTS) tools, so that sitting in a normal office environment in Alaska one can schedule the conference room for meetings while on travel to the Von Braun complex. Likewise, some administrative services are based on DoD-negotiated COTS procurements, such as Microsoft Office for emails, calendars, presentations, spreadsheets, documents, etc.

The MDA CIO office provides general net-centric enterprise services (both unclassified and classified) to MDA supporting the MDA mission for BMDS RDT&E. The general services are based on the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to MDA government and contractor teams. The enterprise general services support such things as globally dispersed Engineering Design Reviews; test readiness reviews; element developmental laboratories technical coordination; test execution; and Executive Management Review Boards. The classified enterprise general services system is considered a 'national security system'.

The MDA CIO has two major data centers, one on Redstone Arsenal, AL (commonly referred to as Huntsville (HSV)) and the other on Schriever Air Force Base (AFB), CO (commonly referred to as Colorado Springs (COS)) both identified as Special Purpose Processing Nodes (SPPN). The HSV data center is predominately the MDA Unclassified Center, and the COS data center is predominately the MDA Classified Center, with each providing disaster recovery, continuity of operations (DR/COOP) services to the other. Concept of Operations (CONOPS) governing the Enterprise utilizes the Information Technology Infrastructure Library (ITIL)

framework and methodologies and a well-defined set of Role Based Administration (RBA) crew categories and responsibilities. The Enterprise CONOPS provides the guidance necessary to manage the increasingly complex computer and network environments while providing customers high quality supported and sustained IT services.

The MDA Enterprise includes but is not limited to: 4 Principal Sites (Fort Belvoir, VA (Headquarters - HQ); Naval Surface Warfare Center Dahlgren Division, VA (Dahlgren - DHL); Redstone Arsenal, AL (Huntsville - HSV); and Schriever AFB, CO (Colorado Springs - COS)), 10 Major Sites, and over 135 Remote Sites connected by Wide Area Network (WAN) Services with over: 260 network enclaves connected to the MDA managed network transport as well as numerous isolated special purpose networked systems; various connections to other DoD networks; 14,000 users with about 18,000 user accounts; 3,000 wireless device users; 2,200 production servers and 400 RDT&E servers; numerous print servers with 1,000 network printers; over 300 VTCs nodes in conference areas and office suites; and VOIP classified and unclassified telephony services.

The MDA CIO office activities related to the administrative and general services net-centric enterprise IT services are: plan, design, acquire, manage, build, populate, operate, protect, defend, maintain, and decommission.

There are many Federal and DoD regulations for implementing ITMA, see paragraph 2.1 below. MDA is a component of DoD. The MDA Director is referred to as a "DoD Component Head" or "Head of DoD Component." The MDA CIO is referred to as a "DoD Component CIO."

2. Organizational Description

The CIO mission is to ensure that MDA information technology services, management and resources are administered, acquired, managed, and operated in compliance with the priorities set by the MDA Director and the goals and directives of existing statutes and DoD regulations. The MDA CIO vision is to provide effective, secure and affordable enterprise information capabilities for missile defense. MDA has standardized the delivery of core enterprise services and applications into eight Service Lines: End User Support, Unified Communications, Cybersecurity Information Assurance (IA)/ Computer Network Defense (CND), Business Automation, Portal & Data Management, Networks and Infrastructure, Data Center, and IT Planning & Solutions. See Figure 2.1 for the MDA CIO Mission, Vision, and Services depiction. MDA CIO strives to deliver integrated services through the eight Service Lines. The MDA SPPN data center configurations are both DoD Architecture Framework (DoDAF) and Joint Information Environment (JIE) compliant and provide processing, storage, and transport of information, human interaction, systems and network management, information dissemination management, and cybersecurity functions.

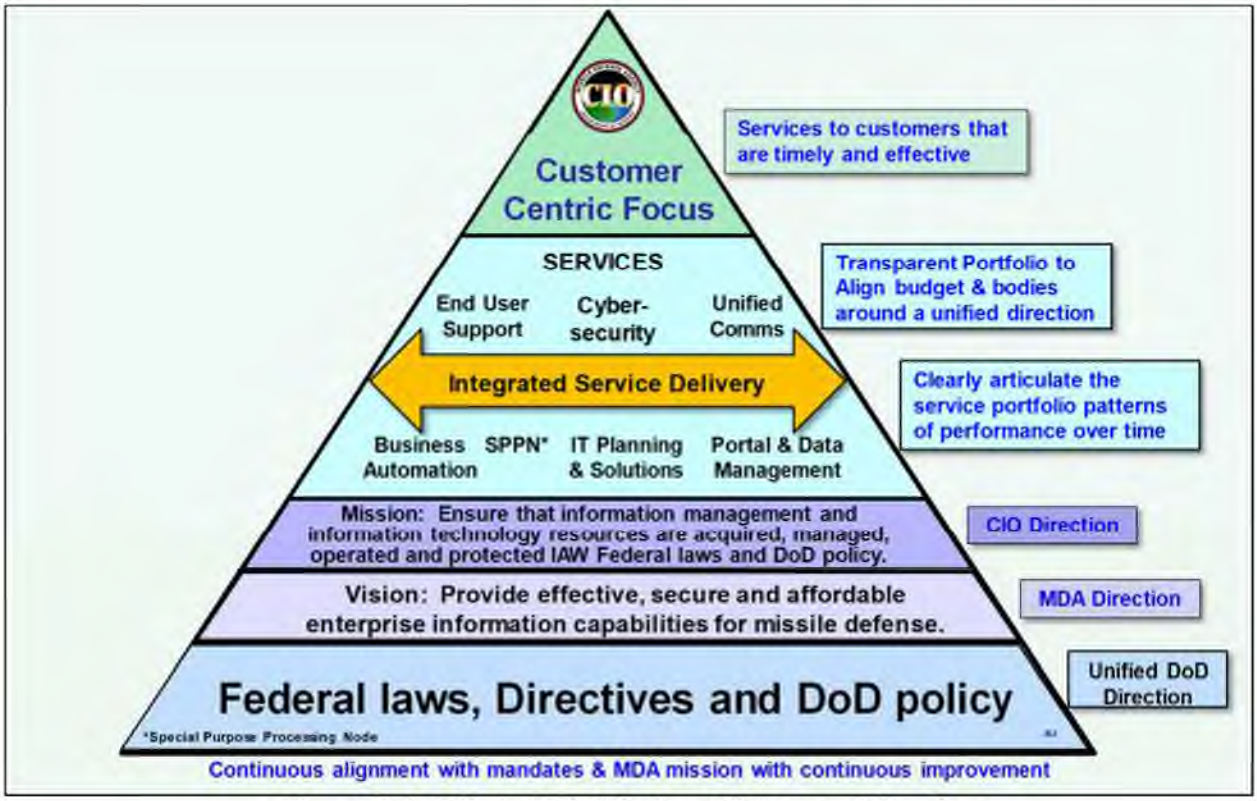


Figure 2.1: MDA CIO Mission, Vision, and Services

The MDA CIO organization is depicted in Figure 2.2. Within the below CIO organization depiction the blue highlighted boxes reflect the associated requirement organizations for this contract.

- Within Figure 2.2 right below the CIO is the Architecture & Engineering (A&E) Team. The A&E Team is part of the CIO organization, comprised of Government and Contractor members. The A&E Team recommends the future MDA Enterprise (SPPN) configuration within the roadmap for implementation. The A&E Team Support requirements are contained in Performance Objective #1.

- Within Figure 2.2 in the middle is the MDA 3-letter organization ICT, Information Management & Technology Operations. The ICT organization oversees the day-to-day execution of the world-wide MDA Enterprise (Admin/GENSER). The ICT requirements are contained in Performance Objectives #3 through #6.

- Within Figure 2.2 in the far right hand column, is the Regional IT Support for the major MDA locations. The Regional IT Support organizations are the CIO's local interface to the MDA workforce. The Regional IT Support requirements are contained within Performance Objective #2.

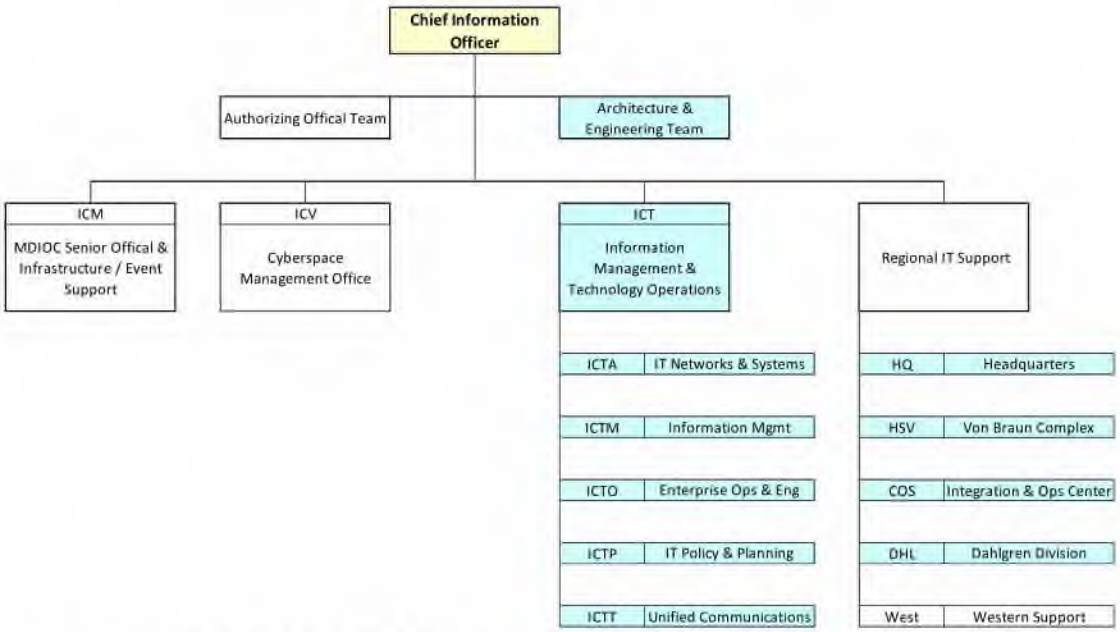


Figure 2.2: MDA Chief Information Officer (CIO) Organization Chart

2.1 Regulatory Guidelines

Specific regulatory guidelines are applicable throughout this requirement for accomplishment of performance objectives in Section 3. The below list identifies the regulatory guidelines and their current version, but the regulatory guidelines associated with this requirement are not limited to the below guidelines, their current version, or superseding regulations.

Regulatory Documentation	
#	Title
1	National Security Presidential Directive, NSPD-23, National Policy on Ballistic Missile Defense, 16 Dec 2002
2	DoDD 5134.09, Missile Defense Agency (MDA), 17 Sep 2009
3	OMB Circular No A-130 Revised, Managing Federal Information as a Strategic Resource, 28 Jul 2016
4	Clinger Cohen Act
5	OMB Memorandum, "Myth-Busting 2": Addressing Misconceptions and Further Improving Communication During the Acquisition Process, 7 May 2012
6	CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 Feb 2011
7	CJCSM 6510.01B, Cyber Incident Handling Program, 10 Jul 2012
8	CNSSP No. 22, Cybersecurity Risk Management, 31 Aug 2016
9	CNSSI No. 1015, Enterprise Audit Management Instruction for National Security Systems, 14 Apr 2016
10	CNSSI No. 1253, Security Categorization and Control Selections for National Security Systems, 27 Mar 2014
11	CNSSI No. 4014, National Information Assurance Training Standard for Information Systems Security Officers, April 2004
12	CNSSI No. 4016, National Information Assurance Training Standard for Risk Analysts, November 2005
13	DoD CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Services, 15 Dec 2014
14	DoD CIO Strategy for Implementing the Joint Information Environment (JIE), 18 Sep 2013
15	DoD CIO Enterprise Service Management Framework, Edition II, 08 Nov 13
16	DoD CIO Information SharingStrategy, 04 May 2007
17	DoD CIO Lifecycle Standards for OSD IT Equipment, 15 Oct 2009
18	DoD CIO Memorandum, Migration to Windows 10 Secure Host Baseline, 20 Nov 2015
19	DoD CIO Memorandum, Delegation of Title 40/CCA Confirmations for Major Defense Automation Program/Major Automation Information Systems Programs, 18 May 2012
20	DoD CIO Memorandum, Department of Defense Commercial Mobile Device Implementation Plan, February 21, 2013
21	DoD CIO Net-Centric Services Strategy, 4 May 2007
22	DoD CIO Net-Centric Spectrum Management Strategy, 3 Aug 2006
23	DoD CIO Net-Centric Data Strategy, 9 May 2003
24	DoD CIO NetOps Strategic Vision, Dec 2008
25	DoD CIO Reference Architecture Description, Jun 2010
26	DoD CIO Memorandum, OMB Strategic Plan for Improving Management of Section 508 of the Rehabilitation Act of 1973, 16 Jul 2013
27	DoD CIO Information Enterprise Strategic Plan, 2010-2012
28	DoD CIO Cloud Computing Strategy, Jul 2012
29	DoD CIO Information Enterprise Architecture (DoD IEA), Version 2.0, Jul 2012
30	DoD CIO Memorandum, DoD Information Enterprise Architecture 2.0, 20 Aug 2012
31	DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, May 2015
32	DoD Cybersecurity Test and Evaluation Guidebook, 1 July 2015
33	DoD Cybersecurity Culture and Compliance Initiative, 30 Sep 2015
34	DoD IEA Version 2.0, Volume I – Management Overview, Jul 2012

Figure 2.3: Regulatory Documentation

Regulatory Documentation	
#	Title
35	DoD Information Resources Management Strategic Plan, Version 1.0, 1 Apr 2015
36	DoD IT Business Case Analysis Template, 22 Oct 2014
37	DoDI 1100.22, Policy and Procedures for Determining Workforce Mix, 12 Apr 2010
38	DoDD 3020.44, Defense Crisis Management, 4 Jun 2007
39	DoDI 3222.03, DoD Electromagnetic Environmental Effects (E3) Program, Incorporating Change 1, 8 Jan 2015
40	DoDD 3600.01, Information Operations (IO), 2 May 2013
41	DoDI 4000.19, Support Agreements, 25 Apr 2013
42	DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 Jun 2004
43	DoDD 4640.13, Management of Base and Long-Haul Telecommunications Equipment and Services, 5 Dec 1991
44	DoDI 4650.01, Policy and Procedures for Management and Use of the Electromagnetic Spectrum, 9 Jan 2009
45	DoDI 4650.10, Land Mobile Radio (LMR) Interoperability and Standardization, July 28, 2015
46	DoDD 4715.1E, Environment, Safety, and Occupational Health (ESOH), 19 Mar 2005
47	DODI 5015.02, DoD Records Management Program, 24 Feb 2015
48	DoDD 5144.02, DoD Chief Information Officer (DoD CIO), 21 Nov 2014
49	DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, 5 Nov 2012
50	DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities, 29 Jan 2010
51	DoDI 5230.24, Distribution Statements on Technical Documents, 23 Aug 2012
52	DoDD 5400.11, DoD Privacy Program, 29 Oct 2014
53	DoDI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance, 14 Jul 2015
54	DoDI 5505.15, DoD Contractor Disclosure Program, 16 Jun 2010
55	DoDI 6055.01, DoD Safety and Occupational Health (SOH) Program, 14 Oct 2014
56	DoDI 7041.04, Estimating and Comparing the Full Costs of Civilian and Active Duty Military Manpower and Contract Support, 3 Jul 2013
57	DoDD 8000.01 Management of the Department of Defense Information Enterprise, February 10, 2009
58	DoDI 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 Apr 2004
59	DoDI 8110.01, Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD, 25 Nov 2014
60	DoDD 8115.01, Information Technology Portfolio Management, 10 Oct 2005
61	DoDD 8140.01 Cyberspace Workforce Management, 11 Aug 2015
62	DoDI 8220.02, Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations, 30 Apr 2009
63	DoDI 8310.01, Information Technology Standards in the DoD, 2 Feb 2014
64	DoDI 8320.02, Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense, 5 Aug 2013
65	DoDI 8320.05, Electromagnetic Spectrum Data Sharing, 18 Aug 2011
66	DoDI 8320.06, Organization Unique Identification (OUID) Standards for Unique Identification of External Department of Defense Business Partners, 26 Sep 2012
67	DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems (NSS), May 21, 2014

Figure 2.3: Regulatory Documentation, continued

Regulatory Documentation	
#	Title
68	DoDM 8400.01-M, Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations, 3 Jun 2011
69	DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 3 Nov 2009
70	DoDI 8440.01, DoD Information Technology (IT) Service Management (ITSM), 24 Dec 2015
71	DoDI 8500.01, Cybersecurity, 14 Mar 2014
72	DoDI 8500.2, Information Assurance (IA) Implementation, 6 Feb 2003
73	DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 Mar 2014
74	DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 24 May 2011
75	DoDI 8540.01, Cross Domain (CD) Policy, 8 May 2015
76	DoDI 8551.01, Ports, Protocols, and Services Management (PPSM), 28 May 2014
77	DoDI 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing, 9 Oct 2007
78	DoDM 8570.01-M, Information Assurance Workforce Improvement Program, 24 Jan 2012
79	DoDI 8580.01, Information Assurance (IA) in the Defense Acquisition System, 9 Jul 2004
80	FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
81	FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
82	FIPS PUB 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2003
83	NIST SP 800-30, Guide for Conducting Risk Assessments, September 2012
84	NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, May 2010
85	NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010
86	NIST SP 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, March 2011
87	NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, 22 Jan 2015
88	NIST SP 800-53A revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations - Building Effective Assessment Plans, December 2014
89	NIST SP 800-60, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
90	NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008
91	NIST SP 800-70 rev 2, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers, February 2011
92	NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, September 2008
93	NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
94	NSAID Net-Centric Enterprise Information Assurance (IA) Strategy Annex to the DoD IA Strategic Plan, Revision 1.0, 26 Apr 2006
95	USD(ATL) Memorandum, Better Buying Power 2.0: Continuing the Pursuit for Greater Efficiency and Productivity in Defense Spending, 13 Nov 2012
96	USD(ATL) Memorandum, Implementation Directive for Better Buying Power 2.0 -Achieving Greater Efficiency and Productivity in Defense Spending, 24 Apr 2013
97	USD(ATL) Fact Sheet, Better Buying Power, Nov 2013

Figure 2.3: Regulatory Documentation, continued

Regulatory Documentation	
#	Title
98	USD(ATL) Memorandum, Update on DoD Implementation Plan for Electronic Subcontract Reporting System (eSRS), 23 Aug 2006
99	USD(ATL) Memorandum, Cash Flow Tool for Evaluating Alternative Financing Arrangements, 27 apr 2011
100	USD(ATL) DoD Efficiencies Key Points 2010
101	USD(ATL) Memorandum, Document Streamlining - Life-Cycle Sustainment Plan (LCSP), 14 Sep 2011
102	USD(ATL) Research and Technology Protection Plans, 30 Jun 2000
103	USD(ATL) Memorandum, Improving the Accessibility of Government Information through Section 508 of the Rehabilitation Act of 1973, as Amended (29 U.S.C. § 794d), 15 Mar 2012
104	USD(ATL) Memorandum, Update to Policy for Unique Identification (UID) of Tangible Items, 3 Sep 2004
105	USD(ATL) Memorandum, Update to Policy for Unique Identification (UID) of Tangible Items New Equipment, Major Modifications, and Reprocurements of equipment and Spares, 26 Nov 2003
106	USD(CPO) Memorandum, Advance Payments to Non-Department of Defense (DoD) Federal Agencies for Interagency Acquisitions, 1 Mar 2007
107	MDA 5013.78-M, Organizational Conflict of Interest, 13 Mar 2013
108	MDA 8000.01-INS, Information Management-Information Technology Investments and Governance
109	MDA 8000.02-DIR, Missile Defense Agency Knowledge Online Portal Management and Operations
110	MDA 8100.02-INS, Wireless Mobile Devices, Date: TBD, 2016
111	MDA 8110.01-INS, Privacy Program
112	MDA 8180.01-DIR, Enterprise Records Management
113	MDA 8190.01-DIR, Electronic Collaboration with Commercial, Educational, and Industry Partners
114	MDA 8260.02-INS, MDA Master Data Catalog
115	MDA Records Management Program and Procedures Guide

Figure 2.3: Regulatory Documentation, continued

2.2 Data Rights

The contractor shall comply with government data rights in accordance with the Defense Federal Acquisition Regulations Supplement (DFARS), as identified below in the PWS and incorporated in the contract:

All technical data (TD) and computer software (CS), algorithms and related models (see DFARS 252.227-7013 and 252.227-7014) to be produced or developed under this contract shall be delivered to the Government with unlimited data rights. The TD and models shall be delivered to the contracting officer in its entirety at any point during the period of performance (POP) of this contract upon written request of the contracting officer or by the end of the contract. The TD and models are to be developed with only Government funds. Do not use open source computer software unless prior written approval is received from the contracting officer. All copyrights for updated and newly developed technical data and models will be assigned to the Government (see DFARS 252.227-7020, incorporated herein).

3. Performance Objectives and Detailed Requirements

Table 3.0 below contains the Performance Objectives Index outlining the objectives to be

performed in accordance with this Performance Work Statement (PWS). Required products for each performance objective shown in Table 3.0 are included within respective PWS paragraphs. While the Performance Objectives align specific activities to IT lines of business, the contractor performance in conjunction with the Government team and other CIO related contracts are to perform as an integrated team, with the MDA workforce defined as the customer. It is the Governments' intent to revise this PWS during the contract period of performance as needed based on, but not limited to: DoD IT and Cybersecurity direction/guidance changes, ever changing cybersecurity threats, IT technology required modifications and upgrades, and/or BMDS RDT&E requirement changes.

Performance Objective Index	Primary Location(s)
1) Architecture & Engineering Team Support	HSV and COS
2) Executive, Regional, and IT Planning Services	HQ, DHL, HSV, and COS
3) IT Networks & Systems Services	HSV and COS
4) Information Management Services	HSV and COS
5) Enterprise Operations & Engineering Services	HSV and COS
6) Unified Communications Services	HSV and COS

Table 3.0: Performance Objective Index and Locations

The following IT Functions listed in Table 3.0.1 below shall be performed in the performance of this effort:

#	IT Functions
1	Perform customer outreach and evaluate customer requirements addressing business/mission needs and evaluate against existing portfolio to determine appropriate solution set
2	Evaluate emerging technologies to determine applicability to MDA RDT&E mission requirements and coordinate inclusion into MDA reference architectures
3	Organize and provide technical advisory and quality assurance across the entire development lifecycle.
4	Ensure enterprise data is leveraged within the MDA data governance model across functional areas in support of Agency missions
5	Evaluate compliance with enclave security requirements in accordance with applicable DoD IA requirements
6	Perform as a technical expert to evaluate proposed and existing architectural solutions

#	IT Functions
7	Evaluate the security of proposed architectural solutions to ensure compliance with DoD regulations, mandates, roadmaps, and policy
8	Perform evaluation and review of proposed IT solutions to ensure the incorporation of DoD directed IA vulnerability solutions, e.g., IAVAs, and provide expert guidance relating to the presence of threats and vulnerabilities should the design be adopted and implemented into the MDA IT Enterprise
9	Review and provide expert analysis of DoD Information Systems (IS) and Platform Information Technology (PIT) systems
10	Perform expert analysis of IA and/or IA-enabled products to ensure compliance with DoD evaluation and validation requirements. (NIAP, APL, Common Criteria, etc…)
11	Provide technical expertise on enclave environment security requirements with applicable DoD cybersecurity requirements to ensure confidentiality, integrity, availability, authentication, and non-repudiation
12	Provide expert recommendations / guidance on best practices to mitigate vulnerabilities on information systems or system components to ensure Risk Management Framework requirements are incorporated into proposed solutions
13	Provide expert support to government contracting officer's technical representatives for associate contractors in the execution and administration of new project and baseline tasks through development of descriptive task language and assisting with government cost estimates, followed by assisting with government technical evaluation and recommendations to the Contracting Officer.
14	Provide expert support to assist the government on quality assurance of the associate contractors' execution of their contracted tasks. MDA/IC has established numerous tasks with incentive fee measurements that require extensive monitoring and management and the TEAMS contractor is expected to assist heavily in this area.
15	Advise and assist the government to improve the operational effectiveness and efficiency of the MDA Office of the CIO in the delivery of IT solutions to the Agency.

Table 3.0.1: IT Functions

3.1 Performance Objective #1: Architecture & Engineering (A&E) Team Support

3.1.1 The contractor shall provide technical expertise to perform the functions identified in Table 3.0.1 for A&E activities in support of Research, Development, Test & Evaluation (RDT&E) oversight while following the regulatory guidance identified in paragraph 2.1 and producing the Key Products/Technical Data identified in paragraph 3.1.11.

3.1.2 The contractor shall conduct research of existing and emerging technological solutions being evaluated or used within the Department of Defense and perform analysis across the Agency's functional areas using demand management patterns to provide recommendations for new capabilities or adjustments to existing capabilities to allow the Missile Defense Agency to gain efficiencies, improve effectiveness, and improve cybersecurity of the IT solutions deployed to our customers and to allow the Office of the CIO to quickly adapt to current and evolving Agency mission priorities.

3.1.3 The contractor shall conduct research of existing and emerging technological solutions being evaluated or used within the Department of Defense and develop a plan for customer outreach to promote and educate customers and stakeholders on the use and value of the Agency enterprise architecture, gather user requirements, determine the gaps between the current and the target architecture, and develop plans for transitioning to target architecture. In this endeavor, the contractor shall develop an understanding of Agency lines of business, how the customers use information technology to address their mission needs, and how innovative technologies can assist the lines of business to be more effective and efficient in the performance of their mission.

3.1.4 The contractor shall provide enterprise architecture guidance, support, and coordination to customers and IT project teams; facilitating technical integration across the IT enterprise by participating in test planning, validation, and reviews.

3.1.5 The contractor shall provide oversight to the MDA CIO Data Governance program to maximize the usability, availability and security of the data used in the MDA enterprise. The contractor shall establish and maintain organizational support for the data governance program and collaborate with stakeholders across the Agency to establish and gain consensus on priorities, standards, definitions, policies and rules associated with ownership and use of Agency information.

3.1.6 The contractor shall provide customer outreach and training to educate business, mission and technical communities on the purpose and benefits of data governance, and assist with obtaining acceptance and adoption of data governance practices; partnering with internal and external business and mission stakeholders to promote solutions that provide strategic value and identify opportunities for improving the quality of shared data assets.

3.1.7 The contractor shall provide A&E technical expertise to monitor and evaluate deliverables of associate contractors. The contractor shall perform research and analysis of emerging and existing technologies and use the results to evaluate A&E technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements. In addition, the contractor shall coordinate and conduct governance and portfolio management activities associated with ensuring compliance with the enterprise architecture for the proffered solutions.

3.1.8 The contractor shall performing expert review of consolidated integrated architecture and engineering solutions and activities to include, but not limited to, a full Enterprise network management analysis with A&E recommendations, a full Enterprise IT systems analysis with A&E recommendations, and a full Cybersecurity analysis with A&E recommendations for the Enterprise unclassified, Secret and Top Secret/Sensitive Compartmented Information (TS/SCI) environments.

3.1.9 The contractor shall prepare and deliver a weekly activity report to the Government and actively participate in recurring coordination meetings; presenting schedules, metrics, technical analysis findings, reports, plans, and roadmap.

3.1.10 A&E Team Support Key Products/Technical Data: technical positions, analysis, findings, recommendations, briefings, and reports; schedules; trip reports; monthly metrics; Executive briefings; and weekly activity report.

Performance Objective #1 Standards		
Objective	**Standard**	**Acceptable Quality Level (AQL)**
A&E Team Support	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.1.1: Performance Objective #1 Standards

3.2 Performance Objective #2: Executive, Regional, and IT Planning Services

3.2.1 The contractor shall provide expert Advisory and Assistance Services to the MDA Office of the CIO in direct support to the MDA CIO as well as support to Regional and IT Planning Services across the MDA IT Enterprise directly supporting the MDA CIO and other IC leaders to deliver IT services, perform customer outreach, collaborate with customers in support of problem resolution, provide quality control initiatives to ensure products and services being delivered by associate contractors meet the governments expectations, are compliant with DoD requirements, and meet the objectives of DoD consolidation initiatives.

3.2.2 The contractor shall provide technical expertise in both Colorado Springs, CO and Huntsville, AL to monitor and evaluate deliverables of associate contractors. The contractor shall perform research and analysis of emerging and existing technologies and use the results to

evaluate technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements.

3.2.3 The contractor shall provide expert advisory and assistance services for regional Enterprise execution and operations; including, but not limited to, identification of concerns and issues, corrective action recommendations, and implementation resolution oversight. The contractor shall perform services listed in Table 3.0.1 for regional leaders and the MDA CIO in support of RDT&E oversight while complying with regulatory guidance.

3.2.4 The contractor shall provide senior IT expertise to advise and assist the government in leading and managing networking, architecture & engineering, enterprise operations, and IT projects across IT functional areas and service lanes to facilitate integrated service delivery, established acquisition timelines, and project synchronization across contracts, across service delivery models, and in compliance with federal mandates and DoD policies. Review service catalog semi-annually and recommend improvements.

3.2.5 The contractor shall perform expert evaluation and review of networks, architecture, engineering, and enterprise operations and progress toward life- cycle maintenance efforts (e.g., analyzing documented requirements, reviewing technical direction letters, and assessing technical evaluations). This includes the review and analysis of other prime contractor technical products and proposed solutions for compliance with MDA and DoD mandates while advising the government of the results.

3.2.6 The contractor shall perform the activities supporting the CIO's Office as part of the MDA/IC organization, the IC Regional Locations, and the MDA Policy and Plans organization, as identified in paragraph 3.2.7, producing the Key Products/Technical Data identified in paragraph 3.2.9.

3.2.7 The Executive, Regional, or IT Planning Services tasks below shall be performed.

3.2.8 The contractor shall perform the following Executive, Regional, and IT Planning Services activities in accordance with the regulatory guidance identified in paragraph 2.1:

a. Day-to-Day. The contractor shall assist in the technical and business operations covering all Executive, Regional, or IT Planning Services activities. Monitor day-to-day execution and operations of current and new networks and systems and provide expert analysis and guidance relating to compliance with DoD roadmaps and consolidation initiatives. Assist with developing strategies and plans, for emerging and future technology initiatives based on the A&E products. Maintain, review, and update processes and procedures.

1) Assist with and provide recommendations on developing Executive, Regional, or IT Planning Services strategy, conducting reviews of existing technologies and systems, reviewing policies Federal, DoD, and MDA guidance, processes, and procedures for CIO related activities.

2) Review and evaluate current configurations, Security Technical Implementation Guide (STIG) / Information Assurance Vulnerability Management (IAVM) checklists, and new technologies for technical soundness, performance, and adherence to standards, plans, goals, and security considerations.

3) Prepare briefings, white papers, information papers, recommendations, governance metrics, and policy assessments.

4) Engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) responses, and maintenance of policy, planning, and investment records.

5) Identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

6) Support the development, maintenance, execution, and monitoring of 2LTR Annual Service Level Agreements (SLA) construct and actual Quarterly IT Service (Core vs Customer) Metrics Reporting by providing the related metrics.

7) Engage in customer identified concerns and present recommendations to the Government Regional Leads.

8) Prepare and submit trip reports.

9) Assist and support MDA Office of the CIO government leads in support of meetings, conferences, presentations, and briefings as requested.

10) Prepare and deliver a weekly activity report covering all Executive, Regional, or IT Planning Services activities.

b. Executive Services. The contractor analyst shall perform the following executive services for the CIO.

1) Maintain/post the CIO IT-related Directives, Policies & Guidance Documents Reference Materials Library on the MDA UMKO and CMKO portal sites.

2) Administer the electronic tasking (E-Tasker) CIO organization unclassified and classified mailboxes for incoming taskers, both from organizations internal and external to MDA, distribute tasking to the correct CIO organization, schedule and monitor tasking response, review tasking response for correct format, coordinate CIO review and approval of tasking response, and once approved distribute response to either internal or external MDA organization.

3) Orchestrate the CIO staff meeting: schedule the meeting, propose the agenda, identify and secure approval of venue for events, prepare and distribute meeting notices, distribute agenda, distribute call for charts containing Internal Controls and DoD reporting metrics, assist with access control, post briefings (shall include executive-level CIO information and/or decision briefings), prepare Executive read-ahead package, facilitate meeting, prepare minutes and action item tracking, post approved minutes to include decisions, track action item closure, and provide recommendation for action item closure. Note: CIO staff includes all CIO organizations both Government and Contractor members. Note: CIO Staff Meeting documentation is posted to the UMKO.

4) Prepare CIO technical and financial briefings, whiteboards, and white papers for CIO communications during executive level meetings and briefings, internal and external to the agency.

5) Maintain currency with DoD guidance, IT technology, and IT business practices. Provide recommendations to the CIO on potential changes based on DoD guidance, IT technology, and IT business practices

6) Draft the overall CIO weekly activity report from across the CIO organization, for CIO communications to other executives.

c. IT Governance and Management Services. As noted in paragraph 3.0, while the Performance Objectives stovepipe specific technical activities, the contractor's performance in conjunction with the Government team and other IT-related contract actions are to perform as an integrated team, with the MDA workforce defined as the customer.

1) Orchestrate the IT Technical Board Meetings. The contractor shall perform administration, quality assurance and oversight management of the MDA IT-related chartered board processes. The contractor shall schedule the meeting; propose the agenda in coordination with the production contractors, identify and secure approval of venue for events (some technical meetings and associated documentation are classified), prepare and distribute meeting notices; distribute agenda; compile production contractor submitted briefings; manage production contractor briefing templates; prepare read-ahead package; facilitate meeting; prepare minutes and action item tracking, secure approval, post approved minutes to include decisions and action items; prepare, secure approval, and distribute Project Champion letter assignments; track action item closure; and ensure board data is populated into respective dashboards. The contractor shall provide monthly status/performance metrics and trending analysis to the Government.

2) Orchestrate the IT Governance Workflows. The contractor shall, on an annual basis, orchestrate the review process of the IT Governance workflows and update the workflows as appropriate. The IT Governance Workflows address: Asset Management, Business Automation Management, Cybersecurity Management, Financial Management, IT Services Management, Privacy and Records Management, Service Level Agreements (SLAs), and Unified Communications; as well as things like E-Tasker and MDA Workforce in-processing. The contractor shall orchestrate the establishment of new workflows based on: the need for more

detailed refinement of a current workflow, DoD IT and/or Cybersecurity direction/guidance changes, and/or MDA oversight/requirement changes. This will also include interaction with Director of Acquisition processes that shall result in IT investments and Services delivery. The contractor shall seek opportunities to support governance workflows related to IT requirements fulfillment associated with any 2 lt requirement or acquisition vehicle.

d. Regional IT Services. The contractor IT/Network specialist shall perform the following activities for their Region.

1) Lead and assist with customer outreach and resolution of IT service issues.

2) Engage in facility workspace management and planning at each region, tracking all local and Enterprise-related proposed changes as well as verifying physical security plans; to include office consolidation and facility infrastructure planning, implementation, and/or migration.

3) Engage and support the acquisition process for unique regional requirements by proactively participating in the MDA chartered Project Steering Committee (PSC) review and approval of the requirements, providing Procurement Initiation Documents (PID) package requirement content, and Engineering and Architecture Board (EAB) reviews of designs and implementations.

4) Monitor, assess, and report monthly the trending metrics by region on: inventory levels, regional project status, open and closed IT request status, and in/out processing moves.

e. IT Policy and Planning Services. The contractor analyst shall assist the IT Policy and Planning office with the overall CIO office Planning, Programming, Budgeting, and Execution (PPBE) processes for the CIO′s portfolio management integration of the CIO approved architecture with the current baseline inventories to identify the investment best mix for Capital Planning and Investment Control (CPIC) while continuously monitoring cost, schedule and performance. While most of the CIO activities support the Enterprise Information Environment (EIE) Mission Area (EIEMA), some CIO activities support the Warfighting Mission Area (WMA) or the Business Mission Area (BMA).

1) Assist with CIO office PPBE activities to include external organization/vendor coordination, such as circuit ordering and billing reconciliation.

2) Perform and provide critical analysis, recommendations, alternatives, and documentation for interface activities to external agencies such as Office of the Secretary of Defense (OSD), Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD(AT&L), High Performance Computer Modernization Program (HPCMP), and the Defense Information Systems Agency (DISA).

3) Assist with CIO office DoD database population, analysis and reporting, ensuring consistency across the DoD IT Portfolio Registry (DITPR), IT Systems Inventory Database, DoD

Information Technology Investment Portal (DITIP), and the Select and Native Programming-Information Technology (SNaP-IT) reporting. Provide DITPR and DITIP Reports. These activities require across organization coordination with the MDA DITPR Administrators, MDA IT Systems Inventory lead, and the respective MDA ISSM/ISSO prior to any modifications. Ensure reported metrics are available for E-Tasker response authors.

4) Assist in collecting and analyzing data and develop IT reports required for DoD, OSD, and Federal government (for example: Organizational Execution Plan (OEP), Data Center Reports, Out of Cycle OEP Responses, Cloud Computing Report, and etc.).

5) Coordinate, prepare, and secure approval for internal agency Service Level Agreements (SLAs) in accordance with the Director's approved IT business rules.

6) Maintain, annually, the SOP to include as a minimum: Collecting Service Line appendix data; Forecasting cost through the Future Years Defense Program (FYDP); Orchestrating 2LTR SLA coordination and Technical Interchange Meetings (TIMs); SLA Finalization Verification with 2LTR; Approval Signature Process (CIO and 2LTR); Distribution of Signed SLA; and Execution of Signed SLA.

f. MDA National, Multinational, and other Conferences Orchestration. The IT/Network Specialist shall orchestrate IT services for conferences and meetings pertaining to networks, architecture, engineering, and enterprise operations at department, Agency, DoD, Federal, and/or private sector meetings. Make recommendations and engage in assigned forums, which include efforts such as reviewing documentations presented, proposing agenda, identifying location, identifying IT configurations and configuration facility and security requirements, assisting with presentations, and preparing for meetings.

1) Maintain annually the SOP to include but not limited to: orchestrate Conference IT requirement coordination; conference planning, scheduling, and acquisition/procurement documentation; conference configuration modification/update staging and testing; and meaningful metrics.

2) Present 120 day-out (120 days prior to conference) Conference briefing on conference plans, configurations, activities, and status.

3) Present 60 day-out Conference briefing on conference plans, configurations, facility preparations, security preparations, activities, and status.

4) Present 10 day-out Conference briefing on conference plans, configurations, facility preparations, security preparations, activities, and status. Track contractor readiness (to include shipments and travel).

5) Provide Conference Report containing as a minimum: metrics, observations, and lessons learned.

3.2.8 Executive, Regional, and IT Policy Support Provider Key Products/Technical Data: SOPs; regionally unique scheduling, monitoring, tracking, and reporting; CIO Staff Meeting announcements, agenda, briefings, minutes, and action item tracking; CIO E-Tasker unclassified and classified mailbox tasking and responses; Executive meeting briefings, whiteboards, and white papers; CIO weekly activity report; Workflows; SLAs; Conference briefings and reports; technical positions, findings, and reports; schedules; trip reports; and monthly metrics.

Performance Objective #2 Standards		
Objective	**Standard**	**AQL**
Executive, Regional, and IT Policy Support	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.2.1: Performance Objective #2 Standards

3.3 Performance Objective #3: IT Networks & Systems Services

3.3.1 The contractor shall provide oversight for Agency Special Purpose Processing Node (datacenter) capabilities supporting flight and ground test, modeling and simulation, and wargame and exercises in support of Agency continuous integration (CI)/continuous agile testing (CAT) requirements. The contractor shall:

a. Partner with internal and external business and mission stakeholders to promote solutions that provide strategic value and identify opportunities for improving the quality of shared data assets
b. Participate in test planning, validation, and reviews to achieve technical integration across the IT Enterprise.
c. Perform needs analyses to define opportunities for new or improved IT solutions supporting the BMDS RDT&E mission aligned to approved Agency Strategic Plans

d. Collaborate with customers to identify and document project requirements and to develop functional and systems requirements and specifications

3.3.2 The contractor shall provide expert assistance with quality assurance and oversight management of a complex network environment that includes multiple local and metropolitan area networks connected through a wide area network that provides centralized and distributed computing and back office resources, multiple security classification levels, and enterprise & local applications. The system services include: Special Access Program IT systems, cross domain solutions (CDS), wide area network program management including Telecommunications Control Office functions, and facility IT buildouts. The contractor shall perform analysis on how to meet user demands for higher reliability and availability of services while meeting DoD requirements.

a. The contractor shall provide technical expertise in both Colorado Springs, CO and Huntsville, AL to monitor and evaluate deliverables of associate contractors. The contractor shall perform research and analysis of emerging and existing technologies and use the results to evaluate IT Networks and Systems technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements.

3.3.2 The contractor shall provide technical expertise to perform the functions identified in Table 3.0.1 for IT Networks and Systems activities in support of RDT&E oversight while following the regulatory guidance identified in paragraph 3.3.3, producing the Key Products/Technical Data identified in paragraph 3.3.4

3.3.3 The contractor shall perform the following IT Networks & Systems Services activities:

a. Day-to-Day. The contractor shall assist in the technical and business operations covering all IT Networks & Systems Services activities. Monitor day-to-day execution and operations of current and new networks and systems. Assist with developing strategies and plans, for emerging and future technology initiatives based on the A&E products. Maintain, review, and update processes and procedures.

1) Assist with and provide recommendations on developing IT Networks & Systems Services strategy, conducting reviews of existing technologies and systems, reviewing policies Federal, DoD, and MDA guidance, processes, and procedures for Enterprise Operations and Engineering.

2) Review and evaluate A&E coordination and changes with current configurations, STIGs/IAVMs, and new technologies, for technical soundness, performance, and adherence to standards, plans, goals, and security considerations.

3) Prepare briefings, white papers, information papers, recommendations, governance metrics, and policy assessments.

4) Engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) responses, and maintenance of policy, planning, and investment records.

5) Identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

6) Support the development, maintenance, execution, and monitoring of 2LTR Annual Service Level Agreements (SLA) construct and actual Quarterly IT Service (Core vs Customer) Metrics Reporting by providing the related metrics.

7) Assist and support CIO, MDA, and DoD meetings, conferences, presentations, and briefings as requested by IC Management.

b. Special Access Program Central Office (SAPCO) Support. Due to the nature of the special access program/sensitive compartmented information facility and program requirements, support to this area requires dedicated advisory and assistance services to produce specified products at higher levels of classification.

1) The SAPCO IT/Network Specialist shall perform the following activities:

a) Assist the government in oversight by assessing the prime contractor's IT Asset and Configuration Management processes using the secure, standalone Defense Property Accountability System (DPAS) instance.

b) Participate in SAPCO weekly meetings and customer requirements meetings to prepare and submit bi-weekly a SAPCO Networks, Architecture, Engineering, and Operations Customer Requirements Engagement Report.

c) Continuously oversee, monitor, and track SAPCO IT contract(s) for cost, schedule, and performance; and provide the program manager with monthly metrics and status.

2) The SAPCO IT/Network Engineer(s) shall perform the following activities:

a) Oversee prime contractor execution of an RMF compliant SAPCO Security Plan per Information System (IS)/Platform Information Technology (PIT) documenting the system categorization: system description to include boundaries, DITPR registration, and assignment of RMF roles. Further details are then added to include: the Common Control Identification as well as identification of the applicable RMF security controls baseline and overall threat environment.

The Security Plan establishes the level of effort required to successfully complete the remaining steps of the RMF process.

b) Oversee the RMF SAPCO Continuous Monitoring Strategy documentation. The System Level IS/PIT Continuous Monitoring Strategy document is submitted with the Security Plan to the SCA for review and comment, and the AO for review, comment, and approval.

c) Provide a monthly status report on the oversight, monitoring, metrics, and tracking of the implementation from the approved cybersecurity controls as outline in the approved Security Plan and Continuous Monitoring Strategy.

d) Based on CCVT data and Security Assessment Report, recommend initial remediation actions to the Program Manager (PM), and initiate a SAPCO IS/PIT POA&M for any controls needing corrective actions.

e) Execute the SAPCO Continuous Monitoring Strategy: re-assess the Security Plan selected controls annually, conduct needed remediation, update Security Plan and POA&M as needed; report SAPCO security status to PM and AO quarterly. As required, repeat step d.

c. Networks and Systems Projects. The IT/Network Specialist(s) shall perform discrete Networks and Systems Project Champion quality assurance and management oversight of A&E defined portfolio projects and/or other MDA 2LTR defined and funded projects. The contractor shall assist in validating customer requirements for the MDA Wide Area Network, and BMDS non-mission communications. Research event details, engage in execution efforts, and implement deployment network engineering guidance to BMDS elements/components for the conduct of agency RDT&E activities such as flight tests, ground tests, and operational deployments worldwide to include Foreign Military Sales.

1) Engage and support the acquisition process by actively participating in the MDA chartered CIO processes: the Project Steering Committee (PSC) review and approval of User requirements, providing Procurement Initiation Documents (PID) package acquisition content, and Engineering and Architecture Board (EAB) reviews of project technical documentation. If project is MDA 2LTR defined and funded, ensure 2LTR coordination throughout the project.

2) Assist with program oversight, quality assurance, and management for project execution and implementation: continuously monitor the RMF cybersecurity controls compliance strategies and implementation; detailed technical and cybersecurity review and analysis of contractor technical products, work products, and deliverables; as well as strategic and tactical planning, program execution (cost, schedule, performance, and risk), life-cycle maintenance efforts, and transition to operations.

3) Review, evaluate, coordinate, schedule, and secure approval of plans for transitioning a technology or new capability from design, development, or pilot mode to operations and maintenance status. Conduct technology transition reviews monthly, evaluate capability, and

make recommendations. In coordination with the respective ISSM/ISSO, facilitate the conduct of externally-driven compliance inspections

d. Facility Outfitting and/or Retrofitting. The IT/Network Specialists shall assist with quality assurance and oversight management for outfitting new and/or retrofitting current facilities with IT and Network initiatives at MDA and/or BMDS sites based on approved plans. The contractor shall:

1) Prepare, maintain, and update the IT/IM Facility Requirements addressing all IT related facility requirements to include but not limited to: communications, HVAC, power, tech power, cable and cable trays, floor-loading, physical security, cybersecurity, and etc. Assist with preparing and reviewing consolidated Facility documentation, requests for proposal, and systems design specifications; based on the IT/IM Facility Requirements, ensure that the IT/IM related requirements are appropriately addressed: communications, HVAC, power, tech power, cable trays, floor-loading, physical security, cybersecurity, and etc. Validate/inspect quality assurance of IT/IM Facility implementations and installations, report findings to Facility Lead and post.

2) Assist in coordinating performance of contracted Enterprise IT and Network outfitting and/or retrofitting facility activities, to include respective ISSM/ISSO cybersecurity reviews at the following (this list will be modified as additional locations are established):

(a) Aegis Ashore Poland
(b) Multiple Upgraded Early Warning Radar (UEWR) site upgrades
(c) Long Range Discrimination Radar Facility
(d) BLDG 247 at Fort Belvoir, VA
(e) Homeland Defense Radar – Hawaii
(f) Consolidated Test Facilities, Huntsville AL

3) Coordinate planning and preparation for approved facility IT decommissioning activities.

4) Coordinate implementation planning for specialty systems.

5) Engage and support the acquisition process by actively participating in the MDA chartered processes: the Project Steering Committee (PSC) review and approval of requirements, providing Procurement Initiation Documents (PID) package requirement content, and Engineering and Architecture Board (EAB) reviews.

6) Evaluate and recommend disposition in conjunction with the IC Directorate property organization. Review accountable assets of existing facility and new requirements affected by agency relocations into new facilities. Evaluate and recommend cleaning, excess property reviews, and disposition, in conjunction with the property accountability organization and the respective ISSM/ISSO.

e. Telecommunications Control Officer. The contractor IT/Network Specialist shall assist in operations of the MDA Telecommunications Office.

1) Monitor, track, and report monthly metrics and status on telecommunications services management: customer requests, circuit analysis, circuit ordering, vendor installation, and circuit quality assurance acceptance.

2) Provide circuit ordering analysis report. In coordination with the customer establish the requirements for circuit utilization, perform analysis of the IT and IM to be supported by the circuit, along with event circuit loading, include average and peak bandwidth expectations, and circuit bandwidth recommendations. Document the analysis findings in a report for review by the wide area network manager and upon approval release and coordination the report with the customer.

3) Submit Order. In accordance with DoD procedures, submit the circuit order. Coordinate with respective Business Financial Manager within the Policy & Plans division and with the customer on the circuit order and the financial requirements.

4) Circuit Acceptance. Verify the usability of the installed circuit; and notify the customer.

3.3.4 IT Networks & Systems Services Key Products/Technical Data: SAPCO SOPs; SAPCO IT Asset and Configuration Management Assessment Report; SAPCO IT/IM Technical Requirements, Cybersecurity, and Architectural Analysis Report; SAPCO Customer Requirements Engagement Report; SAPCO monthly status; Remote Site Active/Inactive Status; monthly metrics; technical recommendations, positions, findings, briefings, and reports; Executive meetings and briefings; weekly activity reports; IT/IM Facility Requirements; Disposition Recommendations; Inspection Findings Report; Telecommunications Circuit Analysis Report; PID packages; Monthly Project Status Report; schedules; trip reports; lessons learned; weekly and monthly services/status/metrics; and weekly activity reports.

Performance Objective #3 Standards		
Objective	**Standard**	**AQL**
IT Networks & Systems Services	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations

Performance Objective #3 Standards		
Objective	**Standard**	**AQL**
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.3.1: Performance Objective #3 Standards

3.4 Performance Objective #4: Information Management Services

3.4.1 The contractor shall, in conjunction with the A&E data governance model, provide technical expertise to advise and assist the government to improve the operational effectiveness and efficiency of the Information Management services through innovative use of data analytics capabilities. They shall advise and assist the government in providing recommendations to improve resilient communications and computing infrastructure by performing the IT Functions listed in Table 3.0.1 and defined in Federal and DoD regulatory guidance.

a. The contractor shall provide technical expertise to advise the government and assist with day-to-day execution and operations of DoD functionally focused Knowledge & Information Management (K&IM) efforts, including classified and unclassified user environments, enterprise applications and database security, data architectures, information libraries and archives, physical and electronic storage of data, data mining capabilities, business processes, privacy act and civil liberties programs, and records management program.

b. The contractor shall provide technical expertise in both Colorado Springs, CO and Huntsville, AL to monitor and evaluate deliverables of associate contractors. The contractor shall perform research and analysis of emerging and existing Information Management technologies and use the results to evaluate technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements

c. The contractor shall assist with strategic and tactical planning, which includes reviewing policies and processes. The contractor shall conduct research of existing and emerging technological solutions being evaluated or used within the Department of Defense and prepare analysis, schedules, diagrams, estimates responses to inquiries, and reports. The contractor shall perform records management activities such as digitizing files, final disposition of content, etc.

and assist with operating a knowledge-based information facility. The contractor shall conduct reviews, audits, and training. The contractor shall engage in reviews, meetings, and conferences.

d. The contractor shall engage and support the acquisition process by actively participating in the MDA chartered processes and assist with program oversight, quality assurance, and management for project execution and implementation. The contractor shall assist with quality assurance and oversight of the Business Automation portfolio. The contractor shall perform Business Automation Project Champion tasks. The contractor shall assist with Data Services specific training and training material development for the following efforts based on approved IT and IM policies and processes. They shall prepare and deliver a Weekly Activity Report covering all Information Management Services activities. The contractor shall engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) to include responses, and maintenance of policy, planning, and investment records. The contractor shall identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

e. The contractor shall perform the IT functions listed in Table 3.4.1 for the Information Management services in support of RDT&E oversight while following regulatory guidance in paragraph 2.1 while executing the tasks in paragraph 3.4.3 and producing the Key Products/Technical Data identified in paragraph 3.4.4.

3.4.2 The IT Functions shall be performed across the MDA IT Enterprise.

3.4.3 The contractor shall perform the following Information Management activities:

a. Day-to-Day. Assist in the technical and business operations covering all Information Management activities. Monitor day-to-day execution and operations of existing and new applications and systems. Assist with developing strategies and plans, for emerging and future technology initiatives based on the A&E products. Maintain, review, and update processes and procedures.

1) Assist with and provide recommendations on developing Information Management Services strategy, conducting reviews of existing technologies and systems, reviewing policies Federal, DoD, and MDA guidance, processes, and procedures for Information Management.

2) Review and evaluate A&E coordination and changes with current configurations, STIGs/IAVMs, and new technologies, for technical soundness, performance, and adherence to standards, plans, goals, and security considerations.

3) Prepare briefings, white papers, information papers, recommendations, governance metrics, and policy assessments.

4) Engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) to include responses, and maintenance of policy, planning, and investment records.

5) Identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

6) Support the development, maintenance, execution, and monitoring of 2LTR annual Service Level Agreements (SLA). Provide the metrics for the Quarterly IT Service (Core vs Customer) Metrics Reports.

7) Engage in the Information Management service delivery to address any customer identified concerns, challenges, limitations, and/or issues and present results and recommendations to the government.

8) Prepare and submit trip reports.

9) Assist and support external meetings, conferences, presentations, and briefings.

10) Prepare and deliver a weekly activity report covering all Information Management Services activities.

b. Data Services. The contractor Technicians shall assist with operating and maintaining the MDA Data Services, generally referenced as Knowledge and Information Tasks Support (KITS), encompassing: MDA Privacy and Civil Liberties, Records Management, Physical Records Inventory, MDA Archives Research, and Publications and Subscriptions; along with the associated training.

1) MDA Privacy and Civil Liberties. Assist with MDA Privacy and Civil Liberties efforts and engage in implementing and communicating approved policies and procedures. Assist with reporting to include technical information for Office of Management and Budget (OMB) reports. Prepare privacy and civil liberties documentation such as Privacy Impact Assessments (PIA), System of Records Notices (SORNs), incident reports, and compliance reports.

a) Maintain annually the SOP to include but not limited to: the annual review of DoD and MDA guidance; MDA guidance update recommendation process; draft incident and compliance reporting (Office of Management and Budget (OMB), Privacy Impact Assessments (PIA), System of Records Notices (SORNs), Civil Liberties Model Program Report, etc.) delivery for review/approval process; training; and the government-contractor roles and responsibilities decomposition.

b) Update and maintain Privacy and Civil Liberties UMKO website/portal sites based on approved materials and/or guidance for all of MDA to access and use.

c) Prepare and submit recommendations for the MDA guidance modifications based on updated Federal and DoD guidance, to the Chief Privacy Officer and/or Civil Liberties Lead for review and approval.

d) Prepare and submit incident, inquiry, and compliance reports, to the Chief Privacy Officer and/or Civil Liberties Lead for review and approval.

e) Provide monthly metrics to the MDA Privacy and Civil Liberties Lead(s).

2) MDA Records Management. Assist with execution and operations of the MDA Records Management Program. Engage in records management, document refresh and updates, and MKO website/portal sites maintenance.

a) Maintain annually, for MDA Records Officer review and approval, the SOP to include but not limited to: Day-to-Day Routine Records Management Activities; the annual review of DoD and MDA guidance; MDA guidance modification recommendation process to include Record Liaison Officers (RLO) procedures; reviewing records management compliance; perform and report on randomly scheduled records management audits; responding to National Archives and Records Administration (NARA) inquiries (contractor drafted, government approval); performing annual self-assessment and OMB/NARA task assessment (contractor drafted, government approval); performing Cybersecurity, Privacy and Information Management evaluations of MDA organizations; digitize and store orphaned records; electronic records management system utilization; training; and monthly electronic records management system reporting.

b) Perform the Day-to-Day Routine Records Management Activities as established in the approved SOPs.

c) Update and maintain Records Management UMKO and CMKO website/portal sites based on approved materials and/or guidance for all of MDA to access and use.

d) Prepare and submit recommendations for the MDA guidance modifications based on updated Federal and DoD guidance, to the MDA Records Officer for review and approval.

e) Perform and report on monthly records management compliance reviews, following the approved SOPs, to the MDA Records Officer for review and approval.

f) Perform and report on records management assessments, audits, and reviews, following the approved SOPs, to the MDA Records Officer for review and approval.

g) Draft official inquiry responses for the MDA Records Officer for review and approval, following the approved SOPs.

h) Perform RLO duties per the agreed to SLA. Establish the continuity of operations plan Vital or Essential Records Package to maintain operations directly after a disaster (natural or man-made).

i) Maintain Records Management artifacts to include but not limited to: file plans, RLO appointment letters, list of trained RLOs, documented exceptions to records management policy, RLO self-inspection results, and schedule validation; following the approved SOPs.

j) Provide monthly Records Management metrics to the MDA Records Officer.

3) Physical Records Inventory. Maintain classified and unclassified KITS inventory, which includes items such as hard copy records, digital tapes, and other physical artifacts such as non-record research products, books, etc.

a) Maintain annually, for MDA Records Officer review and approval, the SOP to include but not limited to: Day-to-Day Routine Physical Records Inventory Activities; inventory declassification; inventory disposition; digitize and catalog hardcopy inventory; electronic and hardcopy record transfer to the NARA; performing an annual cybersecurity review; MDA 2Letter record digitization acquisition recommendations; day-to-day operations of the Huntsville Records Center (records vault);

b) Perform the Day-to-Day Physical Records Inventory Activities as established in the approved SOP.

c) Digitize hardcopy records daily and catalog into the MDA Records Management system, following the approved SOPs.

d) Transfer (arrange for shipment) approved electronic and hardcopy records to the NARA, following the approved SOPs.

e) Provide an acquisition recommendation for other MDA 2Letters records digitization requirements.

f) Operate and maintain the Huntsville Records Center (records vault)

g) Perform and report on physical records inventory assessments, audits, and reviews to the MDA Records Officer for review and approval.

h) Provide monthly Historical Inventory metrics to the MDA Records Officer.

4) MDA Archives Research. Manage classified and unclassified scientific and technical information (STI) to make scientific knowledge and technological innovations are preserved and accessible to MDA policy makers and scientific community.

a) Maintain annually, for MDA STI Officer review and approval, the SOP to include but not limited to: the annual review of DoD and MDA guidance; MDA guidance modification recommendation process; reviewing records management STI identifications; perform and report on periodic searches of STI to define technology baseline, avoid duplication of effort, and justify investment; training; and monthly electronic archive identification and research services metric reporting.

b) Update and maintain MDA Archives UMKO and CMKO website/portal sites based on approved materials and/or guidance for all of MDA to access and use.

c) Assist with STI identification and retrieval from physical and electronic archives.

d) Perform and report on periodic searches of STI records.

e) Providing monthly metrics to the MDA STI Officer.

5) Publications and Subscriptions. Centrally manage MDA ordering of publications and subscriptions leveraging economy of scale, and agency-level consistency in justification and approval. The contractor shall assist with execution and operations of the MDA Publications and Subscriptions Program. Receive customer requests via e-mail, research best value options, and create purchase artifacts such as: Purchase Request forms, Statements of Work, Government Cost Estimates, and Sole Source Justification documents.

a) Maintain annually, for MDA Publications and Subscriptions Lead review and approval, the SOP to include but not limited to: IT Service Request processing; researching best value; and creating acquisition purchase artifacts.

b) Process the IT Service Request for the user requested Publication and/or Subscription.

c) Research procurement options and provide recommendation to the Publication and Subscription Lead.

d) Upon Publication and Subscription Lead approval, create acquisition purchase artifacts.

e) Provide monthly metrics to the Publication and Subscription Lead.

6) Training. Assist with Data Services specific training and training material development for the following efforts based on approved IT and IM policies and processes. Coordinate with the Human Resources Directorate (HR) and provide documentation for participants to receive training credit.

a) Privacy Act Program Training – Privacy annual training content (User, Administrator, Specialist, and Manager) based on policies and related approved topics to implement and communicate program requirements.

b) Civil Liberties Program Training – Civil liberties annual training content based on policies and related approved topics to implement and communicate program requirements.

c) Records Liaison Officer (RLO) Basic Training – The RLO basic monthly training includes file plan development, records inventories, general records policies, customer assessments, and management of active and inactive records in the various IT and IM systems across the agency.

d) RLO Brown Bag Training – Monthly training content based on approved topics from feedback or IC Directorate identified need.

c. Business Automation. The contractor shall perform research on Department of Defense Data Center Optimization Initiatives and Chief Management Office initiatives, provide recommendations and plans on the path forward for outsourcing Defense Business Systems to the maximum extent possible, leveraging DoD-approved cloud service providers. The contractor shall perform quality assurance and oversight of the Business Automation portfolio. The portfolio consists of commercial off the shelf applications and internally custom developed applications. The contractor shall perform Business Automation Project Champion tasks including coordination, quality assurance, and management oversight of A&E defined portfolio projects and/or other MDA 2LTR defined and funded projects.

1) Maintain annually, the SOPs to include but not limited to: the annual review of DoD and MDA guidance; MDA guidance update recommendation process; Business Automation acquisition planning, scheduling, and procurement documentation; DoD Business Automation coordination and reporting; Business Automation modifications/update staging and testing; and meaningful metrics.

2) Prepare and submit the Concept of Operations strategy. Research and analyze emergent IT capabilities, trends, and issues. In coordination with the respective ISSM/ISSO, assist in drafting the Business Automation related Security Plan for the Information System (IS) / Platform Information Technology (PIT) detailing the cybersecurity controls to be addressed.

3) Engage and support the acquisition process by actively participating in DoD, MDA, or other chartered processes: the Project Steering Committee (PSC) review and approval of User requirements, providing Procurement Initiation Documents (PID) package acquisition content, and Engineering and Architecture Board (EAB) reviews of project technical documentation.

4) Assist with program oversight, quality assurance, and management for project execution and implementation: detailed technical and cybersecurity review and analysis of contractor technical products, work products, and deliverables; as well as strategic and tactical

planning, program execution (cost, schedule, performance, and risk), life-cycle maintenance efforts, and operations.

5) Review, evaluate, coordinate, schedule, and secure approval of plans for transitioning a technology or new capability from design, development, or pilot mode to operations and maintenance status. Conduct technology transition reviews monthly, evaluate capability, and make recommendations. In coordination with the respective ISSM/ISSO, facilitate the conduct of externally-driven compliance inspections.

6) Oversee Business Automation modifications/updates installation in a controlled staging area and monitor the integration testing. Provide a Test Observations Report to the Business Automation Lead with your observations, the test results, the controlled staging area definition, and recommendation for migrating to operations.

7) Support Business Automation coordination and reporting to DoD.

d. Portal Services. The contractor Technician shall assist with the quality assurance and oversight management of the MDA Portal Services, to include the UMKO and CMKO portals, 508 Compliance, Dashboards, and MDA public website.

1) Maintain annually the SOP to include but not limited to: the annual review of DoD and MDA guidance; unclassified and classified Portal Services concepts/strategies, utilization, monitoring, and controls; 508 compliance coordination; Dashboard concepts/strategies, utilization, monitoring, and controls; MDA public website concepts/strategies, utilization, monitoring, and controls; annual cybersecurity reviews; and etc.

2) Actively participate in the IT services coordination for both planned and unplanned Enterprise service outages/impacts, ensuring secure operations, establishment of associated escalation process, and change management.

3) Oversee the day-to-day operations and maintenance quality assurance and management of all MDA information management services. Conduct reviews and analysis as req1uested by the government, maximum frequency monthly.

4) Actively participate in IT services coordination, scheduling, monitoring, tracking, and execution of:

- Annual business IT consumption (such as agency annual conferences (MDA, OCONUS International, and Employee Awards)
- Regional events (such as bring your child to work, Organization Day, and etc.)
- BMDS RDT&E exercise and test events
- Perform and document Event Predictive Usage Analysis, present results and recommendations
- Monitor actual event usage for analysis of planned to actual usage.

5) Engage and support the acquisition process by actively participating in the MDA chartered processes: including the Project Steering Committee (PSC) review and approval of requirements, providing Procurement Initiation Documents (PID) package baseline requirement content, and Engineering and Architecture Board (EAB) reviews; as well as other applicable boards and working groups.

3.4.4 Information Management Services Key Products/Technical Data: SOPs; technical recommendations, positions, findings, briefings, and reports; schedules; trip reports; Executive meetings and briefings; MDA Privacy and Civil Liberty recommendations, incident and compliance reports; MDA Records Management recommendations, compliance reports, and assessment/audit reports; Physical Records Inventory reports; Archives Research Search Reports; Training packages; Project Concept of Operations; PID packages; Monthly Business Automation Status Reports; Weekly Service Reports; Event Predictive Usage Analysis; Actual vs Planned Event Usage and Trending Analysis Report; schedules; trip reports; lessons learned; weekly and monthly service/status/metrics reports; and weekly activity reports.

Performance Objective #4 Standards		
Objective	**Standard**	**AQL**
Information Management Services	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.4.1: Performance Objective #4 Standards

3.5 Performance Objective #5: Enterprise Operations & Engineering Services

3.5.1 The contractor shall provide technical expertise to advise and assist with operations of a complex IT environment that includes multiple local and metropolitan area networks connected through a wide area network that provides centralized and distributed computing and back office resources, multiple security classification levels, enterprise and local applications, and public key

infrastructure. The contractors shall engage in design, integration, migration, and implementation of enterprise IT operations, which includes assessing IT and IM systems and applications to meet demands for higher reliability and availability of services. The contractor shall assist with acquiring, developing, and deploying IT services for new facilities; operating and maintaining the existing baseline; and promoting an MDA enterprise environment. The contractor shall provide technical expertise relating to all DoD consolidation efforts, such as datacenter consolidation, to advise and assist the government leadership in development of plans to reach compliance.

3.5.2 The contractor shall provide technical expertise in both Colorado Springs, CO and Huntsville, AL to monitor and evaluate deliverables of associate contractors in support of IC Enterprise Operations & Engineering. The contractor shall perform research and analysis of emerging and existing technologies and use the results to evaluate technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements.

3.5.3 The contractor shall perform the IT/Network Engineer Information Assurance Workforce System Architecture and Engineering functions for the Enterprise Operations and Engineering Services organization in support of RDT&E oversight while following the regulatory guidance identified in paragraph 2.1. The IT/Network Specialist and the IT/Network Engineer, will execute the tasks in paragraph 3.5.4, producing the Key Products/Technical Data identified in paragraph 3.5.5.

3.5.4 The contractor shall provide cybersecurity engineering expertise and oversight of implementations improving Agency defensive cyber operations capabilities. The key tasks associated with this area are:

a. Ensuring the rigorous application of information security/ information assurance policies, principles, and practices to the systems analysis process.
b. Assisting the government in reviewing IT solutions and their implementations for compliance with policies to ensure that systems, network, and data users are aware of, understand, and comply with systems security policies and procedures.
c. Participating in network and systems design reviews to ensure implementation of appropriate systems security policies.
d. Guide and oversee an Enterprise-wide continuous monitoring cybersecurity architecture that meets current DoD monitoring and reporting requirements and ensures alignment and automated reporting of Tier 3 Information Systems (IS) to the accredited MDA Tier 2 Cybersecurity Service Provider CSSP/CERT.

3.5.5 The contractor shall perform the following Enterprise Operations and Engineering Services activities by executing the functions listed in Table 3.0.1, plus the regulatory guidance identified in paragraph 2.1:

a. Day-to-Day. The contractor shall assist in the technical and business operations covering all Enterprise Operations and Engineering Services activities. Monitor day-to-day execution and operations of current and new systems. Assist with developing strategies and plans, for emerging and future technology initiatives based on the A&E products. Maintain, review, and update processes and procedures.

1) Assist with and provide recommendations on developing Enterprise Operations and Engineering Services strategy, conducting reviews of existing technologies and systems, reviewing policies Federal, DoD, and MDA guidance, processes, and procedures for Enterprise Operations and Engineering.

2) Review and evaluate A&E coordination and changes with current configurations, STIGs/IAVMs, and new technologies, for technical soundness, performance, and adherence to standards, plans, goals, and security considerations.

3) Prepare briefings, white papers, information papers, recommendations, governance metrics, and policy assessments.

4) Engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) responses, and maintenance of policy, planning, and investment records.

5) Identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

6) Support the development, maintenance, execution, and monitoring 2LTR Annual Service Level Agreements (SLA) construct and actual Quarterly IT Service (Core vs Customer) Metrics Reporting by providing the related metrics.

7) Engage in the IT services related Customer identified concerns, challenges, limitations, and/or issue resolution coordination, present results and recommendations.

8) Prepare and submit trip reports.

9) Assist and support meetings, conferences, presentations, and briefings as requested.

10) Prepare and deliver a weekly activity report covering all Enterprise Operations and Engineering Services activities.

b. Network and Infrastructure Operations Service Line and End User Service Line Oversight. The IT/Network Specialist shall perform the quality assurance and management oversight of the Network and Infrastructure Operations Services and End User Service Roles Based Administration (RBA) Crews operations and maintenance (O&M) activities by performing the following:

1) Oversee the day-to-day operations and maintenance (networks, infrastructure, end user devices, etc.) quality assurance and management. Conduct reviews and analysis as requested by the government, maximum frequency monthly.

2) Actively participate in the IT services coordination, scheduling, monitoring, tracking, and execution of:

- Annual business IT consumption (such as agency annual conferences (MDA, OCONUS International, and Employee Awards),
- BMDS RDT&E exercise and test events.
- Perform and document Event Predictive Usage Analysis, present results and recommendations.
- Monitor actual event usage for analysis of planned verses actual usage, report.

3) Engage and provide expert technical support to the acquisition of complex IT solutions by actively participating in the MDA chartered processes: the Project Steering Committee (PSC) review and approval of requirements, providing Procurement Initiation Documents (PID) package baseline requirement content, and Engineering and Architecture Board (EAB) reviews; as well as other applicable boards and working groups.

c. Enterprise Engineering Services. The contractor shall perform administration, quality assurance and oversight management of the MDA IT-related engineering lifecycle. The contractor will represent the CIO in Agency IT forums in order to assess the proposed investments in information technology and ensure alignment with DoD mandates and compliance requirements. The IT/Network Engineers shall perform as discrete Enterprise Engineering Project Champion with quality assurance and management oversight of A&E defined portfolio projects, CIO special projects, and/or other MDA 2LTR defined and funded projects:

1) Research and analyze emergent IT capabilities, trends, and issues. In coordination with the Enterprise ISSM/ISSO, draft the Portfolio-Project related Security Plan for the Information System (IS) / Platform Information Technology (PIT) detailing the cybersecurity controls to be addressed.

2) Engage and support the acquisition process by actively participating in the MDA chartered processes: the Project Steering Committee (PSC) review and approval of User requirements, providing Procurement Initiation Documents (PID) package acquisition content, and Engineering and Architecture Board (EAB) reviews of project technical documentation; as well as other applicable boards and working groups.

3) Assist with program oversight, quality assurance, and management for project execution and implementation: continuously monitor the RMF cybersecurity controls compliance strategies and implementation; detailed technical and cybersecurity review and analysis of contractor technical products, work products, and deliverables; as well as strategic

and tactical planning, program execution (cost, schedule, performance, and risk), life-cycle maintenance efforts, and operations.

4) Review, evaluate, coordinate, and schedule plans for transitioning a technology or new capability from design, development, or pilot mode to operations and maintenance status. Conduct technology transition reviews monthly, evaluate capability, and make recommendations. In coordination with the Enterprise ISSM/ISSO, arrange for the Cybersecurity Compliance Tests and Risk Assessments.

3.5.6 Enterprise Operations and Engineering Services Key Products/Technical Data: technical recommendations, positions, findings, briefings, and reports; White Papers; policy assessments; SOPs; Service Level Agreement and IT Services (Core vs Customer) Metrics Report data; Escalation processes; Consolidated Service Report; Event Predictive Usage Analysis; Actual vs Planned Event Usage and Trending Analysis Report; PID packages; Portfolio-Project Security Plan; Monthly Project Status Report; schedules; trip reports; lessons learned; weekly and monthly metrics; and weekly activity report.

Performance Objective #5 Standards		
Objective	**Standard**	**AQL**
Enterprise Operations and Engineering Services	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.5.1: Performance Objective #5 Standards

3.6 Performance Objective #6: Unified Communications Services

3.6.1 The contractor shall provide technical expertise to advise and assist with unified communications services, systems execution, and operations. The contractor shall assist with day-to-day quality assurance and oversight management of: video teleconferencing (VTC),

audio/video services, computer based collaboration services (Skype for Business), wired telephony systems / voice over internet protocol (VOIP), Defense Red Switch Network (DRSN) phones, wireless telephony systems (Blackberries, Androids, and Tablets), and cable plant management. The contractor shall engage in Unified Communications planning and acquisition to include: developing, modifying, reviewing, and analyzing policies, roadmaps, plans, agreements, and security requirements. The contractor shall perform expert analysis and prepare requirements documents, CONOPS, impact statements, briefings, and reports. The contractor shall assist with meeting and conference planning and facilitation. The contractor shall perform and assist with the review of statements of work, cost estimates, and contract language development. The contractor shall develop and assist with the development of Unified Communications systems architecture and planning documentation.

a. The contractor shall provide technical expertise in both Colorado Springs, CO and Huntsville, AL to monitor and evaluate deliverables of associate contractors in support of IC Unified Communications. The contractor shall perform research and analysis of emerging and existing technologies and use the results to evaluate technical designs that are delivered and provide results of the evaluation which will include whether the designs are sound and will implement well into the existing MDA Enterprise Architecture. The contractor will perform quality assurance and quality control of products delivered to MDA to ensure they meet DoD and MDA compliance requirements.

b. The contractor shall perform the activities for the Unified Communications Service organization in support of RDT&E oversight while following the regulatory guidance in paragraph 2.1 while executing the tasks in paragraph 3.6.3, producing the Key Products/Technical Data identified in paragraph 3.6.4.

3.6.2 Any and all of the above defined Unified Communications Services activities shall be executed across the MDA IT Enterprise. The contractor must comply with the BMDS Security Classification Guide (SCG) and the respective element/component unique SCG and Program Protection Plans.

3.6.3 The contractor shall perform the following Unified Communications Services activities in accordance with the regulatory guidance identified in paragraph 2.1:

a. Day-to-Day. The contractor shall assist in the technical and business operations covering all Unified Communications Services activities as well as the systems and architecture design. Monitor day-to-day execution and operations of current and new systems. Assist with developing strategies and plans, for emerging and future technology initiatives based on the A&E products. Maintain, review, and update processes and procedures.

1) Assist with and provide recommendations on developing Unified Communications Services strategy, conducting reviews of existing technologies and systems, reviewing policies Federal, DoD, and MDA guidance, processes, and procedures for Unified Communications.

2) Prepare briefings, white papers, information papers, recommendations, governance metrics, and policy assessments.

3) Engage in daily execution processes, such as classified document accountability, draft electronic tasking (referred to as E-Tasker) responses, and maintenance of policy, planning, and investment records.

4) Identify MDA directives, instructions, manuals, guidance, workflows, and processes impacts and recommended changes required to comply with Federal and DoD guidance and associated reporting.

5) Support the development, maintenance, execution, and monitoring 2LTR Annual Service Level Agreements (SLA) construct and actual Quarterly IT Service (Core vs Customer) Metrics Reporting by providing the related metrics.

6) Prepare and submit trip reports.

7) Assist and support meetings, conferences, presentations, and briefings.

b. Unified Communications Service Line Oversight. The IT/Network Specialist shall perform the quality assurance and management oversight of the Unified Communications Services Roles Based Administration (RBA) Crews operations and maintenance (O&M) activities by performing the following:

1) Actively participate in IT services coordination for both planned and unplanned Enterprise service outages/impacts, ensuring secure operations, establishment of associated escalation process, and change management.

2) Oversee the day-to-day operations and maintenance quality assurance and management. Conduct reviews and analysis as requested by the government, maximum frequency monthly.

3) Actively participate in IT services coordination, scheduling, monitoring, tracking, and execution of:

- Annual business IT consumption (such as agency annual conferences (MDA, OCONUS International, and Employee Awards),
- BMDS RDT&E exercise and test events.
- Perform Event Predictive Usage Analysis, present results and recommendations
- Monitor and document actual event usage for analysis of planned to actual usage

4) Engage and support the acquisition process by actively participating in the MDA chartered processes: the Project Steering Committee (PSC) review and approval of requirements, providing Procurement Initiation Documents (PID) package baseline

requirement content, and Engineering and Architecture Board (EAB) reviews; as well as other applicable boards and working groups.

5) Provide a monthly Service Status Report containing metrics, trending, and recommendations on concerns and issues.

c. Unified Communications Projects. The IT/Network Specialist shall perform discrete Unified Communications Project Champion quality assurance and management oversight of A&E defined portfolio projects and/or MDA 2LTR defined and funded projects:

1) Research and analyze emergent IT capabilities, trends, and issues.

2) Engage and support the acquisition process by actively participating in the MDA chartered processes: the Project Steering Committee (PSC) review and approval of User requirements, providing Procurement Initiation Documents (PID) package acquisition content, and Engineering and Architecture Board (EAB) reviews of project technical documentation; as well as other applicable boards and working groups.

3) Assist with program oversight, quality assurance, and management for project execution and implementation: continuously monitor the RMF cybersecurity controls compliance strategies and implementation; detailed technical and cybersecurity review and analysis of contractor technical products, work products, and deliverables; as well as strategic and tactical planning, program execution (cost, schedule, performance, and risk), life-cycle maintenance efforts, and operations.

4) Review, evaluate, coordinate, schedule, and secure approval of plans for transitioning a technology or new capability from design, development, or pilot mode to operations and maintenance status. Conduct technology transition reviews monthly, evaluate capability, and make recommendations. In coordination with the respective ISSM/ISSO, facilitate the conduct of externally-driven compliance inspections.

5) Oversee Unified Communications modifications/updates installation in a controlled staging area and monitor the integration testing. Provide a Test Observations Report to the Unified Communications Lead with your observations, the test results, the controlled staging area definition, and your recommendation for migrating to operations.

6) Provide a Monthly Unified Communications Project Status Report containing metrics, trending, and recommendations briefing on all enterprise discrete projects from conception to operations.

3.6.4 Unified Communication Services Key Products/Technical Data: technical recommendations, positions, findings, briefings, and reports; White Papers; policy assessments; SOPs; Service Level Agreement and IT Services (Core vs Customer) Metrics Report data; Escalation processes; Consolidated Service Report; Event Predictive Usage Analysis; Actual vs Planned Event Usage and Trending Analysis Report; PID packages; Portfolio-Project Security

Plan; Monthly Project Status Report; Conference briefings and report; schedules; trip reports; lessons learned; weekly and monthly metrics; and weekly activity reports.

Performance Objective #6 Standards		
Objective	**Standard**	**AQL**
Unified Communication Services	Quality – Error-free and technically accurate	No more than two validated customer complaints, in writing, within the monthly reporting period across all locations
	Quality – Compliant with applicable DoD, MDA and local security directives policies, procedures and instructions for safeguarding classified information	Zero validated violations, in writing, within the monthly reporting period across all locations
	Quality/Business Relations – Works independently with minimum corrective action required	No more than two corrective action events within the monthly reporting period across all locations. Note: A corrective action event is when an action is taken, in a corrective manner, due to lower than satisfactory performance
	Schedule – Timely – Meets schedules. Completes actions within specified deadlines	No more than one late or missed scheduled event within the monthly reporting period across all locations

Table 3.6.1: Performance Objective #6 Standards

4. Contract Management

4.1 Limitation of Funds (LOF) and Limitation of Cost (LOC) Notifications

The contractor shall provide the notifications required by FAR Clause 52.232-22, Limitation of Funds, or FAR Clause 52.232-20, Limitation of Cost, by Contract Line Item Number (CLIN). One letter will suffice for multiple CLINs that meet the requirements of the clause(s) within the same time period. In no event shall the cost reports required by Paragraph 4.3 below negate the requirement for required LOF or LOC notifications.

4.2 Monthly Status Report (CDRL A001)

The contractor shall develop and deliver a Monthly Status Report. The report is due the 15th of each month utilizing the format provided as an attachment to the Contract. The status report shall be submitted to the Procuring Contracting Officer (PCO) with a copy to the designated Contracting Officer's Representative (COR), Alternate Contracting Officer's Representative (ACOR), Contracting Officer's Technical Representative(s) (COTR(s)), and the Small Business Office via electronic means. The monthly report shall be a compilation of the Contract Program Manager's weekly activity reports provided to the COTR(s). The report shall include the

following details:

a. Status of required products and services for performance objectives identified in the contract. The contractor shall include as a minimum the monthly schedule delivery metrics for early, on-time, and late deliveries; the monthly metric for personnel security related incidents; monthly metric for predicted deliveries over the next three months; OCI/PCI related FTE metrics; and based on performance feedback, provide monthly metrics on number of corrective action events executed by the Contract Program Manager. The contractor shall identify the product by title and the office that received those products during the reporting period. Delineate those that have been delivered by location, those that are planned to be delivered, and the estimated date of delivery.

b. Status of Other Direct Costs (ODCs). List all ODCs that have been approved by the Contracting Officer. Include by item(s) the approved amount and the actual cost incurred if the purchase has already been made. Also show when the item was received or planned to be received. Segregate the current information and the cumulative information for the applicable CLIN.

c. Submit data in the format provided in the attachment to the contract identifying support for each location identified in the PWS.

d. In accordance with Clause H-09, Organizational Conflict of Interest (OCI), Paragraph f. (2), address 1) the actions taken to discover any actual or potential OCIs; 2) the results of those actions; and 3) actions taken or that will be taken to mitigate any OCIs discovered.

4.3 Cost Report (by CLIN) (CDRL A002)

The Cost Report shall be submitted using the formats provided as attachments to the Contract.

4.4 Travel Status Report (by CLIN) (CDRL A002)

The Travel Status Report shall be submitted using the formats provided as attachments to the Contract.

4.5 Quarterly Self-Assessment

The contractor shall deliver a quarterly self-assessment that addresses contract performance. These quarterly reports are due on the 15th of the month following the end of each quarter from the beginning of the period of performance. The report shall be submitted to the PCO with a copy to the designated COR, ACOR, and COTRs via electronic means. The report shall be in narrative format and address contract performance as defined in Attachment J-09, Quarterly Self-Assessment Report (QSR). All aspects of this contract to include PWS requirements, contract clauses, attachments and delivered products shall be measured during quarterly assessments and subsequently in Contractor Performance Assessment Reports (CPARs). The contractor's self-assessment will not exclude any portions of the contract they believe are relevant to their performance, and all self-assessments with ratings above "Satisfactory" must show what requirement was exceeded and what corresponding benefit to the government was realized in Cost, Schedule, and Performance in either this contract or another BMDS related program/contract vehicle. Contractor shall include this data in the Monthly Status Report

(CDRL A001) at the appropriate time in lieu of a separate QSR.

4.6 Enterprise-wide Contractor Manpower Reporting Application (eCMRA)

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Missile Defense Agency via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported at any time during the FY, all data shall be reported no later than October 31 of each calendar year. Please email the ODC Support Desk with any issues accessing the ODCCMR to the following e-mail address: dod.ecmra-odc-support-desk@mail.mil.

4.7 Small Business

In order to gather data to access the contractor's small business participation IAW FAR 52.219.8 (Utilization of Small Business Concerns) and 52.219-14 (Limitation on Subcontracting), the contractor shall submit a report IAW the Table below, 6 months after contract award and semi-annually thereafter, which provides the actual achievements of small business participation. The contractor shall submit the report as a component of the Monthly Status Report (CDRL A001) only as required by the frequencies identified in this paragraph. The contractor shall submit the report segregated by base period and each option period.

Category	Contractor Name	Product/ Service to Be Performed	Period of Performance	Actual SB Percent of Total Contract	Actual SB Participation Dollars
SB Prime Contractor					
Small Business					
HUB Zone Small Business					
Veteran Owned Small Business					
Service-Disabled Veteran-Owned Small Business					
Small Disadvantaged					
Women-Owned Small Business					

Table 4.7.1 FAR 52.219-8 (Utilization of Small Business Concerns)

ACTUAL CONTRACT LABOR COST (LOADED)	ACTUAL LABOR COST (LOADED) PERFORMED BY THE SB PRIME	ACTUAL PERCENTAGE OF LABOR COST PERFORMED BY THE SB PRIME

Table 4.7.2 FAR 52.219-14 (Limitation on Subcontracting)

4.8 Performance Objectives/Metrics

The Government's assessment of the contractor's performance in achieving the performance objectives contained in this PWS will utilize the standards, acceptable quality levels, and surveillance methods as described herein and in the quality assurance surveillance plan (QASP). Although the criteria and acceptable quality levels of Small Business, Cost, Management, and Regulatory Compliance are not specifically included in the PWS; the overall performance assessment will include these criteria.

4.9 Identification of Contractor Employees

All contract personnel attending meetings, answering Government telephones and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

4.10 IA Workforce Management Report (A007)

The contract shall implement the DoD 8570.01-M C7 IA workforce management requirements, to include, but not limited to: management review of IA workforce positions; managing personnel training, certificates, and certifications; managing acknowledgement of understanding and responsibilities and privileged access agreements; and DoD reporting. DoD 8570.01-M requires DoD Components to manage the DoD contractors reporting of contractor personnel IA certification status and compliance with DoD 8570.01-M. The contractor shall prepare and submit a monthly IA Workforce Management Report CDRL meeting the required content as defined in DoD 8570.01-M for both the IA workforce to position metrics and individual personnel baseline certifications qualifications.

4.11 Monthly Manpower Report (A006)

The contractor shall develop and deliver a Monthly Manpower Report using the format provided as an attachment to the contract. The report shall be submitted to the Procuring Contracting

Officer (PCO), the Contracting Officer's Representative (COR), and the COTR(s) 30 days after contract award and subsequently on the last work day of each month thereafter.

5.0 Cybersecurity Risk Management

The contractor shall safeguard and protect Controlled Unclassified Information (CUI) provided by or generated for the Government (other than public information) that transits or resides on any non-Government information technology system. Information shall be protected from unauthorized access, disclosure, incident or compromise by extending the safeguarding requirements and procedures in DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. The NIST 800-53 security controls specified in 252.204-7012 shall be extended to include CUI information which resides on, or transits through the contractor's (prime and all sub-contractors) unclassified information technology systems.

6.0 Security Requirements

This contract requires access of classified information up to and including Top Secret. The Contractor shall be required to obtain a Top Secret Facility Clearance within a reasonable time as to not affect contract performance and their employees requiring access to classified information shall be eligible to possess a security clearance commensurate with the level of information for which they require access. All contractor personnel requiring unescorted access to MDA/BMDS facilities shall be required to possess and maintain a minimum of a Secret security clearance. The Contractor shall defer to the Contracting Officer for their representative(s) for classified access requirements.

Eligibility is defined as the formal determination that an individual meets the Personnel Security requirements for Access to a specified type or types of classified information.

Contractor individuals that require access to SCI shall have a Top Secret Personal Clearance with SCI eligibility (had been formally indoctrinated for SCI within the last 24 months).

The security clearance level requirement will be monitored by the Government upon contract award and during contract execution. Refer to Section J - DD Form 254 for additional contract security requirements.

7.0 Travel and Other Direct Cost (ODC) Requirements

a. Contractor employees shall expect to travel from 10% to 25% of the time to various locations to include manufacturing sites, integration sites, and test sites. Locations will be within the contiguous United States (CONUS) or outside the contiguous United States (OCONUS).

b. Requests for Contractor Travel (MDA Form 110) shall be submitted at least 17 days in advance of travel when possible. This is to allow the contractor to secure the most advantageous

rates.

c. The Contractor shall use the Synchronized Pre-deployment and Operational Tracker (SPOT) web-based system, to enter and maintain data for all Contractor personnel that are authorized to accompany U.S. Armed Forces and/or U.S. Government personnel OCONUS.

d. ODCs are anticipated for this contract.

e. Travel within the local area or base of assignment to attend meetings, conferences, seminars or perform work shall be considered a cost of doing business and shall not be separately reimbursed as a travel expense. Local area travel is defined as a 30 mile radius around the duty location or designated place of performance.

f. Travel to Republic of Korea (ROK)

Contractors may be required to travel to the ROK. U.S. Government Contractors who travel to ROK must be identified as Invited Contractors/Technical Representatives (IC/TR) in accordance with United States Forces Korea (USFK) Regulation 700-19 (The Invited Contractors and Technical Representatives Program) to be provided coverage under the US/ROK Status of Forces Agreement (SOFA). In order to obtain SOFA status in Korea, the Contractor employees shall present a DOD identification card obtained stateside prior to travel, passport with A-3 Visa and SOFA stamp, Letter of Authorization, and a red-stamped USFK Form 700-19A-R-E to Korean immigration authorities upon request.

The Responsible Officer (RO) or ACOR will inform the PCO of any anticipated Contractor travel to Korea as soon as the requirement is known. The RO will coordinate with the contractor to prepare and submit a complete USFK Form 700-19-A-R-E and supporting documentation to USFK/FKAQ no later than 30 business days prior to travel. Contractor travel is not authorized until USFK/FKAQ has approved Part III of the USFK Form 700-19A-R-E. Timely responses to requests for information from the RO are critical to ensuring requirements are met in time to support travel.

Training Requirements for IC/TR personnel shall be conducted in accordance with USFK Reg 350-2 Theater Specific Required Training for all Arriving Personnel and Units Assigned to, Rotating to, or in Temporary Duty Status to USFK. IC/TR personnel shall comply with requirements of USFK Reg 350-2. The RO will provide necessary instructions for accessing and completing this training.

8.0 Government Furnished (GF) Materials (GFM), Information (GFI), and Equipment (GFE)

8.1 Facilities

a. The Government will provide office facilities, equipment, and materials for daily business use. This includes office space, desk/work station, telephone, chair, computer, printer, and requisite consumable materials. The contractor shall abide by the MDA standard operation procedures (such as opening and closing procedures) associated with the provided office facilities and equipment. For contracting purposes, at each location a Regional IT Support member will be identified as the contract site lead for Emergency Recall notification, Facility Emergency Evacuation coordination, and the like.

b. The Government will provide keys or codes for access to Government facilities. These keys and codes shall be controlled, tracked, and protected. Upon termination of the period of performance, all keys, codes, access badges, or other government furnished equipment (e.g., cell phones, computers, etc.) shall be returned in accordance with MDA Instruction 1400.06-IN.

Location	Number of work stations*
Redstone Arsenal, AL	19
Schriever AFB, CO	21
Ft. Belvoir, VA	1
Dahlgren, VA	1

Table 8.1: Onsite GFE per Location

* This table will be completed upon award.

8.2 Government Furnished Equipment (GFE)

a. The contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment (GFE) or Contractor-Acquired-Government Owned Property (CAP).

b. The inventory accounting system must specify, as a minimum, product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The contractor shall either attach an updated inventory report to each monthly status report or certify that the inventory has been updated and is available for Government review. In either case, the contractor's inventory list must be available for Government review within one business day of Procuring Contracting Officer (PCO) or COR request.

c. The contractor shall contact the Directorate of Logistics (DPL) Centralized Property Office (CPO) for proper use of Government vehicles on site and temporary duty (TDY), extreme cold weather kits, use of Military Aircraft to travel to remote locations and other logistics support requirements not identified in this PWS.

8.3 Government Furnished Information (GFI)

The Government will provide access to all information necessary to perform tasks associated with activities outlined in this contract.

8.4 Government Furnished Property (GFP) Reporting Requirements

Government Furnished Property (GFP) is not anticipated in the course of execution of this contract.

9.0 Transition and Staffing

a. The contractor shall fill positions according to the functional areas and timelines identified in Table 9.0 below.

b. Key personnel for this effort are the Contract Program Manager and Technical Leads. The Transition Period begins on the first day of period of performance. The Transition Period ends 14 calendar days after start of period of performance.

c. The Contract Program Manager and Technical Lead(s) shall meet with the COR, ACOR, COTRs, and Functional Integrator (FI) or their designated representative within 5 working days of the start of the Period of Performance as part of the transition and Contract Kickoff Meeting. The Contract Program Manager and/or Technical Lead shall report the status of its efforts to recruit, hire, and fill all positions within the timeline specified in Table 9.0 at the Contract Kickoff Meeting. The contractor shall submit clearance paperwork for hires upon award to immediately begin the physical and network access processes. At the Contract Kickoff Meeting the Government will provide the Contractor with: the technical configuration as of the contract initiation, classified content related to the contract execution, technical performance monitoring and feedback, BMDS training coordination details, MDA Action Officer training coordination details, arrange specific SCI and SAP read-ins, and the facility office arrangements. The Contract Kickoff Meeting technical discussions will be held at the Secret security classification level with specific (need-to-know) SCI and SAP data provided to program specific employees that have been read-in.

Staffing Area	Timeline
Contract Program Manager	At start of Period of Performance
Technical Lead(s)	At start of Period of Performance
Staff to perform all Performance Objectives	By end of Transition Period

Table 9.0: Transition and Staffing Requirements

d. Table 9.1 maps the contract staffing from contract labor category to DoD 8570.01-M IA Workforce categories to this ITMA PWS Performance Objectives and the associated security clearance requirements.

Contract Labor Category	IA Workforce Category	Performance Objectives	Security Clearance
Contract Program Manager	N/A	Contract Program Manager	TS
Technician (Advanced)	IAT III	#4 Information Management Services	Secret
Technician (Intermediate)	IAT II	#4 Information Management Services	Secret
Engineer (Advanced)	IASAE III	#1 Architecture & Engineering (A&E) Services #5 Enterprise Operations & Engineering Services	TS
Engineer (Intermediate)	IASAE II	#1 Architecture & Engineering (A&E) Services #3 IT Networks & Systems Services	TS/SCI
Specialist (Advanced/Intermediate)	N/A	#2 Executive, Regional, and IT Planning Services #3 IT Network& Systems Services #5 Enterprise Operations & Engineering Services #6 Unified Communications Services	Secret
Analyst (Advanced)	N/A	#2 Executive, Regional, and IT Planning Services	Secret
Analyst (Intermediate)	N/A	#2 Executive, Regional, and IT Planning Services	Secret
Analyst (Basic)	N/A	#2 Executive, Regional, and IT Planning Services	Secret

Table 9.1 Staff Mapping

e. No On-The-Job (OTJ) skills practical evaluations are planned.

10.0 Option Requirements

All requirements for the option years will be executed as defined by the above requirements. The option requirements will include all approved modifications made to the contract throughout the period of performance.

Surge Support for Mission Requirements: Surge capability may be required during non-core hours to support Government authorized mission priorities at CONUS or OCONUS locations. This support may require personnel to work extended hours, to include weekends. The tasks to be performed are contained in the technical performance objectives and will be within the current contract period of performance. Upon Government request, the contractor shall provide, within 2 business days, a cost estimate which will be used to obtain funding and to exercise a portion of the option CLIN. Prior to surge effort being performed, authorization from a PCO must be achieved by modification to the contract.