MISSILE DEFENSE AGENCY

DEPARTMENT OF DEFENSE

C2BMC Spiral Capability Development Contract

C2BMC Operations & Maintenance, Logistics, Warfighter Integration, and Deployment

Task Order Number 0013

Rev 7

7 December 2017

Table of Contents

1.0 Background

This Task Order (TO) provides Operations & Maintenance, Integrated Logistics, CoCom Integration, Deployment, and Disposal of the Command and Control, Battle Management and Communications (C2BMC) to the fielded systems. This effort is a follow-on and continuation of the Sustainment and Warfighter Integration effort provided under HQ0147-12-D-0003, Task Order 9 - Operations & Maintenance, Task Order 10 - Sustainment, and Task Order 11 – Deployment.

2.0 Technical Expert Status Accreditation (TESA)

The Contractor shall adhere to the requirements of the Army in Europe Regulation AE 715-9 to ensure compliance with the TESA related requirements.

2.1 For Contractor personnel serving in an Area of Responsibility (AOR) that requires TESA and in accordance with Department of Defense Instruction (DoDI) 3020.37, "Continuation of Essential DoD Contractor Services During Crises," effective January 26, 1996, overseas positions supporting the Contingency Architecture Activation Team effort in [redacted] and other overseas positions supporting MDA under this Contract, the Contracting Officer hereby designates the following positions/job functions as Emergency/Mission Essential:

(b)(3):10 U.S.C. § 130

a. United States European Command (EUCOM) Operations and Sustainment (O&S) Lead/Technical Expert (TE)
b. Architecture and System Engineering (A&SE) COCOM Site Engineer/TE
c. BMDS Network Operations and Security Center (BNOSC) Network Engineer/TE
d. Information System Security Officer (ISSO)/TE
e. Network Engineer, BMDS Communications Network (BCN)/TE
f. Operations and Sustainment Team Watch Stander/TE
g. Operations and Sustainment Gateway Operator/TE
h. WF EUCOM Liaison Officer (LNO)/TE

2.2 Only the Contracting Officer can designate specific positions as Emergency/Mission Essential and any new designation shall be made in writing by the Contracting Officer by modification to the SOW. Once a position is designated as Emergency/Mission Essential, the Contractor personnel filling that position shall be considered Emergency/Mission Essential on his or her Defense Department Form -1172-2 and Common Access Card (CAC).

2.3 In accordance with paragraph 6.7 of the DoDI 3020.37, the Contractor shall develop contingency plans for tasks performed by Emergency/Mission Essential personnel to provide reasonable assurance of continuation during crisis conditions and deliver these plans via the Data Accession List (DAL).

3.0 Program Management

The Contractor shall provide Program Management services to assist the Government in planning, controlling, directing, monitoring, reporting, and managing for this Task Order (TO).

The Contractor shall establish a Failure Review Board (FRB), to determine root cause and ensure timely corrective action for critical failures, when requested by the Government.
All documentation created and maintained in a database or storage medium associated with this contract shall be delivered to the Government by the various Contract Data Requirement List (CDRL) associated with this contract. All deliverables (CDRLs) shall be submitted to the Government electronically, unless otherwise stated, with distribution method to the Government to be determined by the C2BMC Program Management Office (PMO).

3.1 Integrated Process and Product Development (IPPD)

The Contractor shall apply an IPPD approach in all technical/functional disciplines and requirements in a coordinated effort to meet established financial management, resource, cost, schedule, performance, and supportability requirements for the C2BMC system.

3.2 Contractor Integrated Performance Management

The Contractor shall prepare and utilize, in the performance of this TO, an integrated performance management system. Central to this integrated system shall be a Department of Defense (DoD) validated Earned Value Management System (EVMS). The EVMS shall be linked to, and supported by, the Contractor's management processes and systems to include the Integrated Master Schedule (IMS), Contract Work Breakdown Structure (CWBS), change management, material management, procurement, cost estimating, and accounting.

3.3 Integrated Baseline Reviews (IBRs)

The Contractor shall engage jointly with the Government's program manager and their representatives in IBRs to evaluate the risks inherent in the contract's planned performance measurement baseline for this TO. The totality of the baseline shall be reviewed and evaluated no less than annually by the Government. Each IBR shall verify that the Contractor is using a reliable performance measurement baseline (to include the entire contract scope of work for this TO), is consistent with contract schedule requirements, and has adequate resources assigned.

3.4 Process Control

The Contractor shall maintain a set of operating documentation that provides management direction, policies and procedures, per established contractor tools and procedures in accordance with (IAW) existing Government processes.

3.5 Program Reviews

The Contractor shall support the planning, preparation, conduct, and preparation of minutes of program reviews. The Contractor shall support the IBR, Program Management Reviews (PMR), Synchronization of Program Execution Activity Roundtable (SPEAR), Government Internal Configuration Control Board (ICCB), Integration Synchronization Group (ISG)/Integration Synchronization Center (ISC), Program Change Board (PCB), In Progress Reviews (IPR), the Training Configuration Management Board (TCMB) and bi-weekly Joint Business Reviews (JBR), and other relevant meetings as requested and/or agreed upon by the Government. The Contractor shall support C2BMC component immersion reviews with the Government to facilitate understanding and agreement with implementation approaches used for chosen technical efforts. The results of these reviews shall include updating project documentation based on the outcome of the reviews.

3.6 Bills of Material Management (BOM)

The Contractor shall manage the BOM and control changes IAW program configuration control procedures for this task order. The Contractor shall monitor new material requirements and identify when changes are required to BOM line items to meet baseline program requirements.

3.7 Quality, Safety and Mission Assurance Management

In accordance with the Quality Assurance Program Plan, the Contractor shall provide Quality Engineering support for the design, assembly, build-out, installation and test of the following deployment activities identified in Section 7.0 Deployment. The Contractor shall comply with the System Safety Program Plan and the Environmental, Safety and Occupational Health Plan for activities included in this task order.

4.0 Operations & Maintenance

4.1 Level I On-Site Operations & Maintenance:

The Contractor shall provide operations and maintenance support to C2BMC operational, test, and training systems at all C2BMC locations IAW Appendix A, the staffing & response times in Appendix A, and to the availability levels specified in the MDA System Specification (Classified). The Contractor shall perform Preventive Maintenance Inspections (PMIs) on all C2BMC operational, test, and training systems at all locations IAW Appendix A based on vendor recommended intervals and procedures and/or actual operating experience. The Contractor shall adhere to international agreements and site-specific procedures while performing operations and maintenance. The contractor shall provide 24/7 security operations for the (b)(3):10 U.S.C. § 130 site listed in Appendix A, adhering to local (b)(3):10 U.S.C. § 130 physical security standards.

4.2 C2BMC Control Center:

The Contractor shall provide a C2BMC Control Center (CCC) to manage and execute all operations, system administration, system/network monitoring, cyber defense and maintenance activities for all C2BMC operational, test, and training equipment at sites identified in Appendix A.

The Contractor shall coordinate with Cyber Protection Teams, MDA Computer Network Defense Service Provider (CNDSP) / Computer Emergency Readiness Team (CERT), BMDS Tier 2 CNDSP, and BMDS Tier 3 CNDSPs concerning security incident handling IAW Chairman Joint Chiefs of Staff (CJCS) 6510-01M, MDA Authorizing Official (AO) direction, and STRATCOM/JFCC-IMD direction to ensure comprehensive security of C2BMC.

4.3 Level II Maintenance (Help Desk):

The Contract CCC shall provide Level II maintenance and help desk support for all C2BMC operational, test, and training equipment at sites identified in Appendix A.

4.4 Information System Security Officers (ISSOs):

The Contractor shall fulfill the duties and responsibilities of an ISSO IAW DoDI 8500.01 Cybersecurity, dated March 14, 2014, and supplemented by the Information System Security Manager (ISSM) in the ISSO appointment letter, as outlined in Appendix E for associated locations and systems specified in Appendix C-6. The Contractor shall report the Cybersecurity Program status during two monthly meetings with the Government ISSM. The Contractor shall support and attend quarterly Cybersecurity planning / training meetings as scheduled by the Government ISSM. The Contractor shall supply monthly Cybersecurity risk charts for the C2BMC Executive Risk Board. The Contractor shall provide and document Incident Response Procedures (IRP), Disaster Response (DR) and Continuity of Operations Procedures (COOP) training to C2BMC O&M crews annually (CDRL A124). The Contractor assigned ISSOs shall attend, or participate via telecom, two additional monthly staff meetings with the Government ISSM.

5.0 Integrated Logistics Support:

5.1 Logistics Support

The Contractor shall maintain a supportability strategy and conduct integrated logistics support for existing and planned U.S. and International C2BMC hardware/software. The Contractor shall provide integrated logistics support to C2BMC operational, test, and training systems at all locations IAW Appendix A, the staffing & response times in Appendix A, and to the availability levels specified in the MDA System Specification (Classified). The Contractor shall ensure that the system is supported and available through its life-cycle. The Contractor shall participate in planning of potential deployment scenarios and provide recommendations for support alternatives and identify risks and issues. The Contractor shall accomplish Integrated Product Support Planning. The Contractor shall provide ILS engineering during production and deployment activities of C2BMC systems. ILS support shall be provided for the C2BMC systems integration, testing, and certification and accreditation at deployment locations. The contractor shall maintain and update/keep current a supportability strategy via an Integrated Logistics Support Plan, site specific support plans, and supportability assessments for system modifications and development. The contractor shall conduct a semi-annual ILSWG.

5.2 Supply Chain Management:

The Contractor shall provide supply chain management to C2BMC operational, test, and training systems at all locations IAW Appendix A, the staffing & response times in Appendix A, and to the availability levels specified in the MDA System Specification (Classified). The Contractor shall maintain a logistics management information system. The Contractor shall ensure hardware and software supply chain security iaw corporate processes.

5.3 Sustaining Engineering

5.3.1 Reliability, Availability, and Maintainability (RAM):

The Contractor shall update/keep current the RAM program plan that describes RAM program, RAM model, RAM metrics, and integration with C2BMC ticketing system, preventative maintenance inspections, and obsolescence engineering. The Contractor shall perform Reliability, Availability, and Maintainability (RAM) analysis for C2BMC system listed in Appendix A and provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development. The Contractor shall support the BMDS Joint Reliability and Maintainability Evaluation Team (JRMET) process, Data Scoring Board (DSB), Operational Test Agency (OTA), and BORRS. The Contractor shall assess and identify root cause for all C2BMC Discrepancy Reports (BDRs) within 60 calendar days of assignment by MDA FRACAS Board. The Contractor shall provide all supporting data, analysis, and objective evidence associated with BDR root cause assessment.

5.3.2 Obsolescence Engineering:

The Contractor shall perform Obsolescence Engineering/End of Life/End of Sale analysis for C2BMC systems listed in Appendix A and provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development. The Contractor shall conduct a Material Review Board for material that is discrepant, obsolete, or excess as required.

5.3.3 Cybersecurity Engineering:

The Contractor shall conduct Cybersecurity IAW requirements, guidance, policies, and procedures in the overarching IDIQ in "Applicable Documents" and in Appendix B titled "Cybersecurity Guidance", (CDRL A052 and A124). The Contractor shall conduct Cybersecurity for C2BMC Mission, Test, Training and Planning Systems associated with the continued operations of the fielded systems; (b)(3):10 U.S.C. § 130
(b)(3):10 U.S.C. § 130

5.3.3.1 Risk Management Framework

The Contractor shall plan, conduct, and manage the C2BMC RMF in accordance with (IAW) Appendix B, Appendix D, and Government templates (CDRL A095, A057, A124). The Contractor shall initiate and/or transition and maintain Risk Management Framework (RMF) package(s) for C2BMC operating locations IAW Cybersecurity Guidance Documents in Appendix B, Appendix D, and C2BMC Program Protection Plan (CDRL A095, A057, A124). The Contractor shall utilize the C2BMC Program Protection Plan and leverage materials existing in the MDA Classified Enterprise Mission Assurance Support System (eMASS) and create additional policies, procedures and artifacts to meet RMF requirements. The Contractor shall start with BMDS Critical Controls as identified in Appendix D and continue with remaining controls identified in NIST SP 800-53. The Contractor shall provide variance information as required for non-compliant BMDS Critical Controls by 30 September 2016.

5.3.3.1.1 RMF Architecture

The Contractor shall ensure any new C2BMC system requirements, specifications, architectures, and designs are IAW Appendix B. The Contractor shall conduct change management IAW the Contractor CM Program to ensure that changes and modifications made to the C2BMC's security architecture are evaluated, tested and captured in architecture, design, test, and A&A documentation in eMASS IAW CDRL A124. The Contractor shall use internal CM processes as described in the C2BMC Systems Engineering Plan to evaluate and approve Cybersecurity related changes. The Contractor shall document these Cybersecurity architectures in the form of architecture drawings to include sufficient descriptive data to support decision makers and provide architectural drawing(s) updates as approved changes are implemented (CDRL A124). The Contractor shall assess, analyze, update documentation and provide technical changes as appropriate for the SW/HW compliance to include End of Support / End of Service / End of Life issues. The Contractor shall recommend cybersecurity architecture strategy changes for government approval and will include C2BMC Control Center (CCC) in the architecture. The Contractor shall update a System Security Plan and Systems Security Guides as required after system updates (CDRL A124).

5.3.3.1.2 RMF Authorization Maintenance

The Contractor shall obtain and maintain authorizations and connection approvals necessary to sustain C2BMC operations, training/exercises, and testing as applicable. The Contractor shall maintain site-specific Cybersecurity IRP, DR and COOPs in eMASS and site specific plans and procedures and document review annually. The Contractor shall maintain and update packages as required, but no less than annually. The Contractor shall submit the artifacts via eMASS 60 days prior to operational requirement and submit monthly updates to the artifacts package as required. The Contractor shall correct, mitigate, or submit risk acceptance package of all CAT I (DIACAP), Very High, and High (Risk Management Framework (RMF)) findings within 30 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all CAT II (DIACAP) and Moderate (RMF) findings within 90 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all CAT III (DIACAP), Low, and Very Low (RMF) findings within 180 days. The Contractor shall update existing DIACAP packages in eMASS, as required, until transition to RMF packages in eMASS are complete; to ensure cybersecurity authorizations do not lapse.

5.3.3.1.3 RMF Plan of Action and Milestones (POAMs)

The Contractor shall upload a monthly vulnerability auto-scan database as designated by the Government. The Contractor shall develop Plan of Action and Milestones (POA&M) IAW Appendix B, Appendix D, and Government templates and timelines. The Contractor shall maintain and update the eMASS POA&Ms as needed, but no less than quarterly. The Contractor shall maintain an internal database to reconcile accuracy of C2BMC cybersecurity risks and provide the government monthly POA&M status. The Contractor shall maintain an internal data base, as required, as a means to verify and reconcile the accuracy of C2BMC vulnerabilities and for cyber program management activities.The Contractor shall generate reports and artifacts to support the MDA Designated Approving Authority (DAA's) C&A / A&A processes, FISMA reporting, and MDA Executive Risk Board (A124).

5.3.3.2 Cybersecurity Engineering

The Contractor shall conduct Systems Security Engineering in accordance with Industry Best Practices and those guidelines provided in Appendix B. The Contractor shall support Government related engineering meetings, forums, boards as required to ensure that Cybersecurity is adequately and properly integrated. The Contractor shall report on the progress of engineering in the monthly progress report. The Contractor shall provide support during the installation and checkout of all cybersecurity related upgrades, patches and modifications to the system baselines. The Contractor shall evaluate all CTOs, COTS vendors patches, security alerts, vulnerabilities announcements (IAVMs, OPORDS, EXORDS, WARNORDS), DoD, NIST and MDA policy updates, system monthly scan results, , physical and system vulnerability assessments, and continuous monitoring program findings for C2BMC systems listed in Appendix A. The Contractor shall provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development and shall update POAMs. The Contractor shall conduct Cybersecurity risk management IAW the Contractor internal risk program and risk approaches as agreed with the Government ISSM. The Contractor shall take assessment results for incorporation in IA releases as approved by the Government and update the IAVM/Patch Management Plan accordingly (CDRL A124). The Contractor shall provide IA releases to the C2BMC architecture on a quarterly basis for Mission and Test/Training/Planning systems, and monthly for Administrative systems (i.e. CIMS/Tivoli). The Contractor shall update all engineering artifacts and associated documentation as required. The Contractor shall attend internal working groups and boards to respond to cybersecurity alerts and announcements.

5.3.3.3 Cybersecurity Tools

The Contractor shall manage the Network Defense Capability with respect to Cybersecurity monitoring, security operations, operational software tools, and computing hardware requirements. (b)(3):10 U.S.C. § 130 The Contractor shall perform monthly system security scans/tests on all systems identified in Appendix A. The Contractor shall upload scans into a database approved and accessible by the government and evaluate within 30 days of receipt of findings. The Contractor shall develop technical solutions and report in accordance with the program management planning/processes/procedures. The Contractor shall plan for and execute procedures for the development and execution of changes due to events according to the Notice Event Analysis and Response process. The Contractor shall utilize a Single Sign-On capability allowing the user to access resources as authorized by their role with a single set of authorized credentials. The Contractor shall ensure the architecture requires the user to re-authenticate as they traverse security and/or technology boundaries to establish different permissions within the different portions of the system and to accommodate disparate technologies where automatic credential exchange is not possible.

5.3.4 Reserved

5.3.5 Warfighter Requirements:

The Contractor shall perform engineering and analysis of Warfighter Improvement Process (WIP) submittals and provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development.

5.3.6 Continuous Improvement Program (CIP):

The Contractor shall implement and maintain a Continuous Improvement Program (CIP) by soliciting ideas for improvement from employees and government. The Contract shall coordinate with the Government on CIP project selection and prioritization. The CIP will not supplement or augment the System Modification Request (SMR) process, but instead will focus on support tool, process, and quality of life improvements.

5.3.7 External/Internal System Configuration Changes:

The Contractor shall perform engineering analysis for externally driven interface and/or configuration changes for C2BMC systems listed in Appendix A to include GFX M&S tools and provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs) (via the Data Accession List). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development.

5.3.8 Software Modification Requests (SMRs)/Troubleshooting Procedures (TPs):

The Contractor shall develop and test SMRs/TPs resulting from RAM engineering, Obsolescence engineering, cybersecurity engineering, warfighter requirements, and external interface/configuration changes as prioritized by the Government. The Contractor shall provide a description of the test approach (via the Data Accession List) and pass/fail criteria for development. The Contractor shall present SMR/TP test and pass/fail results at ICCB prior to fielding.

5.3.9 Level III Maintenance (SME Reachback):

The Contractor shall provide scheduled and/or unscheduled off-site maintenance SME reachback support for equipment in Appendix A to restore the system to operational status when repair is beyond the capability of on-site personnel. The Contractor shall provide telephonic support for the fielded TSS Software.

6.0 CoCom Integration:

6.1 Liaison Officers (LNOs):

The Contractor shall provide dedicated on-site LNOs for CENTCOM and EUCOM. The Contractor shall provide rotating LNO's in support of NORTHCOM/ STRATCOM, MDA Ft. Belvoir/NMCC and MDA Huntsville. The Contractor LNO shall maintain up-to-date knowledge and documentation of COCOM-specific doctrine, plans, C2 structure and C2 execution, TTPs, etc., as it pertains to the use and contribution of C2BMC operations to that COCOM. The Contractor shall ensure that all LNO's maintain C2BMC SME status. The Contractor LNO shall ensure that COCOM HQ staff is updated and briefed on all C2BMC system and SME involvement in wargames, exercises, test events, and operational events.

6.2 Training Delivery:

The Contract shall maintain training material and conduct up to 16 training classes per year in CONUS and OCONUS locations. The Contractor shall provide advanced training in Missile Defense operations, Sensor Management, GEM Operations, and Planner for both operators and subject matter experts.

6.3 Training Scenario:

The Contractor shall troubleshoot, modify, and/or develop up to 15 scenarios per year.

6.4 Subject Matter Experts:

The Contractor shall maintain the C2BMC SME Program, to include the administration, certification, event coordination, training, scheduling, and publishing an event final report. Upon Government request, the Contractor shall provide C2BMC SMEs at locations participating in the exercises, test events, wargames, training events, or target of opportunities/real world events. The Contractor SMEs shall be cognizant of all C2BMC functionalities performed during the event and submit inputs for all requested report information upon event completion. The Contractor shall establish a Planning Support Cell to provide tailored training and SME support to the Warfighter. The Contractor SMEs shall support development, modification and loading of operational, test, exercise, and training defense design for the fielded systems for EUCOM, CENTCOM, STRATCOM/JFCC-IMD, NORTHCOM, and PACOM. The Contractor SMEs shall provide defense design briefs and participate in working groups as directed by the Government. The Contractor shall provide planner SME and technical support for operational Planner locations and program office support in Huntsville & MDIOC. Planner support shall include analysis and experimentation as directed. Modifications to the C2BMC SME Program must be approved by the Government.

6.5 Demonstrations, RFIs/RFAs, Assessment Activities, Real World Events/ Contingency Operations

The Contractor shall update and provide demonstrations of C2BMC capability as directed in both classified and unclassified venues for U.S. and allied military and civilian agencies. The

Contractor shall execute special emphasis tasks that include implementation of technical study results or recommendations; requests for analyses, requests for information, assessments, and reports; issue resolutions for C2BMC; procurement of material; software updates/engineering releases; and facility changes.

The Contractor shall support Cyber Assessments (i.e., ECRE, SCAs, Color Teams, COCOM assessments) through TIMS, Working Groups, and deployment of assessment support personnel.

The Contractor shall maintain flexibility to call upon various degrees and types of support. Support could entail supporting mission priorities, real world deployments, and contingency events both CONUS and OCONUS. Results shall be delivered to the Government IAW instructions in the Task Instruction(s).

7.0 Major Deployments, Minor Deployment, and System Configuration Changes:

For each major deployments, minor deployments, and system configuration changes, the Contractor shall provide a test plan to the Government for approval IAW requirements for these capabilities. The contractor shall address any risk areas presented by the system changes and identify any risks associated with test limitations. After government concurrence of the test plan, the contractor shall assist in the EOW so that assets and BMDS elements can be scheduled. The test plan shall be presented early enough to meet the initial submittal requirement of an EOW into the asset management process. The contractor shall provide daily status reports (DSRs) on the progress of the software installation, integration and field test activities in sufficient detail for the government to assess progress and direct/concur with the release of the system back into operations. The contractor shall update CDRLs, technical documentation, Government furnished and Contractor acquired property lists, architecture & cyber security artifacts, training material, and provide training on approved configuration changes as appropriate (CDRLs A052, A095). The contractor shall document the results of software field testing in a Summary Briefing to the government NLT 2 weeks after conclusion of the test. This briefing shall document the actual activities performed, the achievement of the test objectives, any open issues and SMRs, lessons learned and any recommendations for future testing.

For major and minor deployments, the Contractor shall support a Deployment Readiness Review (formerly known as Hardware Ship Readiness Review) that shall encompass deployment site and equipment readiness. For major and minor deployments, the Contractor shall support an Operational Readiness Review (ORR) that will occur during soak periods and formally establish the “as-built” baseline for the new site/equipment.

7.1 System Configuration Changes:

The Contractor shall install and test configuration changes, approved by the PERB, ICCB, TCMB, ISG, and/or PCB. The contractor shall keep test and training system configurations consistent with operational system configurations. The Contractor shall support externally driven configuration changes.

7.2 Minor Deployment: CENTCOM Flexible Scenario Capability:

The Contractor shall upgrade the CENTCOM DTS with the flexible scenario capability developed for the EUCOM S6.4 DTS. The Contractor shall provide ability to reconfigure CENTCOM DTS connections.

7.3 Minor Deployment: BTG Safety Upgrades:

The Contractor shall provide BTG safety upgrades in NORTHCOM, PACOM, and EUCOM. The Contractor shall also continue engineering efforts to support the future CENTCOM implementations.

7.4 Decommissioning and Retrograde of Equipment:

A decommissioning plan shall be developed and provided to Government for approval to support the decommissioning and retrograde Spiral 6.4 equipment in Appendix A. This plan shall address restocking of equipment as spares and disposal of all C2BMC equipment in Appendix A. The Contractor shall decommission CDIN 1 after FTG 15 by removing usable equipment for spares.

8.0 Cybersecurity

The Contractor shall execute the types of tasks identified (but not limited to) within this section (8.0 of this Statement of Work). This effort is a LOE best effort construct and will be closely managed by the Task Order leads and SMEs on both the government and contractor teams. The Contractor shall conduct Cybersecurity IAW requirements, guidance, policies, and procedures in the overarching IDIQ in "Applicable Documents" and in Appendix B titled "Cybersecurity Guidance", (CDRL A124). The Contractor shall conduct Cybersecurity for C2BMC Mission, Test, Training and Planning Systems associated with the implementations and maintenance of the fielded systems.

The Contractor shall engineer an approach to providing an integrated C2BMC health and status Common Operating Picture (COP) to include system operational status, system cyber status, circuit operational status, trouble ticketing status, and estimated time to return to operations capability. Delivered via the DAL.

8.1 Cybersecurity Engineering

The Contractor shall conduct Systems Security Engineering in accordance with Industry Best Practices and those guidelines provided in Appendix B. The Contractor shall ensure that Cybersecurity requirements have been identified and incorporated into system design. The Contractor shall support Government related engineering meetings, forums, boards as required to ensure that Cybersecurity is adequately and properly integrated into system design. The Contractor shall evaluate all CTOs, COTS vendors patches, security alerts, vulnerabilities announcements (IAVMs, OPORDS, EXORDS, WARNORDS), DoD, NIST and MDA policy updates, system monthly scan results, physical and system vulnerability assessments, policy updates for Cycle 2, GTX/Early Integration (EI), GTI, GTD Cycle 5 Test Results, Cyber Protection & Color Team Findings, STIG Applicability Matrix (SAM) (annually), and Cybersecurity Tool Effectiveness (annually) and continuous monitoring program findings for C2BMC systems. Based on these evaluations, the Contractor shall provide the Government a risk/opportunities assessment with recommended Courses of Actions (COAs). The Contractor shall submit the COA selected by the Government into the System Modification Request (SMR) process for prioritization and development and shall update POAMs. For Spiral 8.2-3, the Contractor shall take assessment results for incorporation in IA releases as approved by the Government, update the IAVM/Patch Management Plan accordingly (CDRL A055), and provide IA releases to the C2BMC architecture on a quarterly basis for Mission and Test/Training/Planning systems, and monthly for Administrative systems (i.e. CIMS/Tivoli). The Contractor shall report on the progress of engineering in the monthly progress report.

8.2 Risk Management Framework

The Contractor shall plan, conduct, and manage the C2BMC RMF in accordance with (IAW) Appendix B, Appendix D, and Government templates (CDRL A095, A124). The Contractor shall initiate and or transition and maintain Risk Management Framework (RMF) package(s) for C2BMC operating locations IAW Cybersecurity Guidance Documents in Appendix B, Appendix D, and C2BMC Program Protection Plan (CDRL A095, A124). The Contractor shall submit RMF packages (e.g. NORTHCOM package includes Mission Node, DTS Node, User Node, UK Rel, Element Node, BTG, and applicable GFX equipment) and deliver in eMASS per Government approved schedule. The Contractor shall utilize the C2BMC Program Protection Plan and leverage materials existing in the MDA Classified Enterprise Mission Assurance Support System (eMASS) and create additional policies, procedures and artifacts to meet RMF requirements. The Contractor shall start with BMDS Critical Controls as identified in Appendix D and continue with remaining controls identified in NIST SP 800-53. The Contractor shall provide variance information as required for non-compliant BMDS Critical Controls by 30 September 2016.

8.2.1 RMF Authorization Maintenance

The Contractor shall obtain and maintain authorizations and connection approvals necessary to sustain C2BMC operations, training/exercises, and testing as applicable. The Contractor shall maintain and update packages as required, but no less than annually to meet continuous monitoring requirements. The Contractor shall submit the artifacts via eMASS 60 days prior to operational requirement and submit monthly updates to the artifacts package as required. The Contractor shall correct, mitigate, or submit risk acceptance package of all Very High, and High (Risk Management Framework (RMF)) findings within 30 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all Moderate (RMF) findings within 90 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all Low, and Very Low (RMF) findings within 180 days.

8.2.2 RMF Plan of Action and Milestones (POAMs)

The Contractor shall conduct monthly scans and upload into vulnerability auto-scan database as designated by the Government. The Contractor shall develop Plan of Action and Milestones (POA&M) IAW Appendix B, Appendix D, and Government templates and timelines. The Contractor shall maintain and update the eMASS POA&Ms as needed, but no less than quarterly. The Contractor shall maintain an internal database to reconcile accuracy of C2BMC cybersecurity risks and provide the government monthly POA&M status. The Contractor shall maintain an internal data base, as required, as a means to verify and reconcile the accuracy of C2BMC vulnerabilities and for cyber program management activities. The Contractor shall generate reports and artifacts to support the MDA Designated Approving Authority (DAA's) C&A / A&A processes, FISMA reporting, and MDA Executive Risk Board (A124).

8.3 Cybersecurity Assessments

The Contractor shall support C&A, A&A, Cyber Protection Team (CPT), Color Team (e.g. Red/Blue/Green), ECRE, and COCOM assessment required activities, to include TIMS, Working Groups, and deployment of assessment support personnel. The Contractor shall coordinate with Assessment and CPTs, MDA CNDSP / CERT, BMDS Tier 2 CNDSP, and other BMDS Tier 3 CNDSPs to ensure the comprehensive security of the BMDS. The Contractor shall provide operational cybersecurity support to deployment/fielded site locations to include artifacts in eMASS IAW guidance in CDRL A124, IAVA compliance, CTOs, Site Assistance Visits (SAVs), Security Controls Assessment (SCA) findings, CND, and system modifications.

9.0 Period of Performance

16 December 2015 through 19 January 2018.

10.0 Task Order Monitor

The Procurement Contracting Officer (PCO) will provide a letter identifying the names of the primary/alternate Task Order monitors.

11.0 Travel

The Contractor shall travel as necessary to participate in meetings, conferences, program reviews, technical interchanges, and test events to accomplish the work described in this task order.

12.0 Deliverables

The following Contract Data Requirements List (CDRL) identifies the required deliverables for this task order. Copies of the CDRLs can be found in the base IDIQ Award, Exhibit A. The

Master Contract Deliverables Requirements List (CDRL) identifies the required deliverables associated with this Task Order.

CDRL #	**CDRL Title**
A057	DIACAP Package
A052	System Security Concept
A093	C2BMC Operational Readiness Report
A095	PPS Registration
A124	System Security Plan
A055	Patch Management Plan

13.0 Government Furnished and Contractor Acquired Property

All Government Furnished items (GFx) associated to this task order are identified in "Attachment 4 - Government Furnished Information/Services/Facilities/Pending Property" and "Attachment 9 Master Government Property List" of the Basic Contract.

14.0 Places of Performance

All places of performance associated with this task order are identified in Section 12.0 of “Attachment 1 – Contract Statement of Work” of the Basic Contract.

15.0 Acronym List

ACRONYM	**CALL OUT**
ABOX	Automated BMDS OPIR Translator
A&A	Assessment and Accreditation
BMD	Ballistic Missile Defense
BMDS	Ballistic Missile Defense System
BOA	BMDS OPIR Architecture
BOM	Bills of Material
BORRS	Ballistic Missile Defense System Operational Readiness Reporting System
C2	Command and Control
C2BMC	Command and Control, Battle Management and Communications
COA	Course of Action
CCC	C2BMC Control Center
CDIN	C2BMC Deployed Interface Node
CDRL	Contract Data Requirements Line
CENTCOM	US Central Command
CERT	Computer Emergency Readiness Team
CIP	Continuous Improvement Program
CJCS	Chairman Joint Chiefs of Staff
CNDSP	Computer Network Defense Service Divider
COCOMs	Combatant Commands
COMSEC	Communications Security
CONOPS	Concepts of Operations
CONUS	Continental United States
CSSC	C2BMC System Support Center
DAA	Designated Approving Authority
DD	Defense Department
DMETS	Distributed Multi-Echelon Training System
DoD	Department of Defense
DoDI	Department of Defense Instruction
DRR	Deployment Readiness Review
DSB	Data Scoring Board
DTS	Distributed Training System
EUCOM	European Command
EVMS	Earned Value Management System
EWS	Enterprise Work Stations
GEM	Global Engagement Manager
GFE/ GFI	Government Furnished Equipment/ Information
GFP	Government Furnished Property
GFX	Government Furnished Other
GOTS	Government Off The Shelf Software

HQ	Headquarters
IA	Information Assurance
IAW	In Accordance With
IBR	Integrated Baseline Review
ICCB	Internal Configuration Control Board
IMF	Index Mapping File
IMS	Integrated Master Schedule
IPPD	Integrated Process and Product Development
ISC	Integration Synchronization Center
ISG	Integration Synchronization Group
ISSOs	Information System Security Officers
JFCC-IMD	Joint Forces Command Center – Integrated Missile Defense
JRMET	Joint Reliability and Maintainability Evaluation Team
LNO	Liaison Officer
LRDR	Long Range Discrimination Radar
MCCC	MAJCOM Communications Coordination Centers
MCS	Mission Control Station
MCSB	Mission Control Support Backup
MDA	Missile Defense Agency
MDIOC	Missile Defense Integration and Operations Center
MOA(s)	Memorandum of Agreement(s)
M&S	Modeling and Simulation
NIST	National Institute of Science and Technology
NLT	No Later Than
NMCC	National Military Command Center
NORTHCOM	Northern Command
O&M	Operations and Maintenance
O&S	Operations & Sustainment
OCONUS	Outside Continental United States
OMF	Optimistic Modeling Framework
OPORDS	Operations Order
OPIR	Overhead Persistent Infra-Red
OTA	Operational Test Agency
ORR	Operational Readiness Review
PACOM	Pacific Command
PCB	Program Change Board
PCO	Procurement Contracting Officer
PERB	Program Engineering Review Board
PMIs	Preventative Maintenance Inspections
PMO	Project Management Office
POC	Point of Contact
PPS	Ports, Protocols, and Services
QA	Quality Assurance

RAM	Reliability, Availability, and Maintainability
RMF	Risk Management Framework
SBIRS	Space Based Infrared System
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SMR	System Modification Request
SOW	Statement of Work
STOC	System Test and Operations Center
STRATCOM - OFFUTT	Strategic Command - Offutt Air Force Base
TO	Task Order
TSS	Training System Sustainment
TTPs	Test, Training, and Procedures
VAFB	Vandenberg Air Force Base
WF	Warfighter

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

(b)(3):10 U.S.C. § 130;(b)(7)(E)

[redacted]

(b)(3):10 U.S.C. § 130;(b)(7)(E)

Appendix B: Cybersecurity Guidance

CJCSI 6510.01F	**Information Assurance (IA) and Computer Network Defense**
CNSSI 1253	Security Categorization and Control for National Security Systems and applicable overlays found in 1253F Attachments
DoD Memorandum	Open Source Software in the Department of Defense
DoDM 5200.01, Vols 1-4	DoD Information Security Program (All 4 Volumes)
DoDD 5200.2	DoD Personnel Security Program
DoDD 8140.01	Cyberspace Workforce Management
DoDI 8500.01	Cybersecurity
DoDI 8510.01	Risk Management Framework (RMF) for DoD Information Technology (IT)
DoDD 8530.1	Computer Network Defense (CND) Directive
DoDI 8551.01	Ports, Protocols, and Services Management (PPSM)
DoD 8570-01-M	Information Assurance Workforce Improvement Program
DoD 8580.1	Information Assurance (IA) in the Defense Acquisition System
MDA Inst 8430.01-INS	Software Acquisition
MDA Plan 8500.02-P	Information Assurance Program Plan
NIST SP 800-27 A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
NIST SP 800-37	Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-64	Security Considerations in the System Development Life Cycle
NIST SP 800-70	National Checklist Program for IT Products—Guidelines for Checklist Users and Developers
NIST SP 800-127 A	Engineering Principles for Information Security Technology
NIST SP 800-	Continuous Monitoring
NIST SP 800-	System Security Engineering
STIGS	All Applicable DISA STIGS

Appendix C-6: ISSO Locations

Locations	On Site	Off Site
(b)(3):10 U.S.C. § 130	X	
[redacted]	X	
[redacted]		X
[redacted]	X	
[redacted]		X
[redacted]	X	
[redacted]		X
[redacted]	X	
[redacted]	X	
[redacted]		X
[redacted]		X
[redacted]		X
[redacted]	X	X
[redacted]		X

Appendix D: BMDS Critical Controls

ID	Title
AC-2	Account Management
AC-2(1)	Account Management | Automated System Account Management
AC-2(2)	Account Management | Removal of Temporary / Emergency Accounts
AC-2(3)	Account Management | Disable Inactive Accounts
AC-2(4)	Account Management | Automated Audit Actions
AC-2(5)	Account Management | Inactivity Logout
AC-2(7)	Account Management | Role-Based Schemes
AC-2(9)	Account Management | Restrictions on Use of Shared Groups / Accounts
AC-2(10)	Account Management | Shared / Group Account Credential Termination
AC-2(11)	Account Management | Usage Conditions
AC-2(12)	Account Management | Account Monitoring / Atypical Usage
AC-2(13)	Account Management | Disable Accounts For High-Risk Individuals
AC-6	Least Privilege
AC-6(1)	Least Privilege | Authorize Access to Security Functions
AC-6(2)	Least Privilege | Non-Privileged Access For Nonsecurity Functions
AC-6(3)	Least Privilege | Network Access to Privileged Commands
AC-6(5)	Least Privilege | Privileged Accounts
AC-6(7)	Least Privilege | Review of User Privileges
AC-6(8)	Least Privilege | Privilege Levels For Code Execution
AC-6(9)	Least Privilege | Auditing Use of Privileged Functions
AC-6(10)	Least Privilege | Prohibit Nonprivileged Users from Executing Privileged Functions
AC-17(4)	Remote Access | Privileged Commands / Access
AC-17(6)	Remote Access | Protection of Information
AC-17(9)	Remote Access | Disconnect / Disable Access
AT-2	Security Awareness Training
AU-11	Audit Record Retention
AU-11(1)	Audit Record Retention | Long-Term Retrieval Capability
AU-2	Audit Events
AU-2(3)	Audit Events | Reviews and Updates
AU-3	Content of Audit Records
AU-6	Audit Review, Analysis, and Reporting
AU-6(1)	Audit Review, Analysis, and Reporting | Process Integration
AU-6(10)	Audit Review, Analysis, and Reporting | Audit Level Adjustment
AU-6(3)	Audit Review, Analysis, and Reporting | Correlate Audit Repositories
AU-6(4)	Audit Review, Analysis, and Reporting | Central Review and Analysis
AU-6(5)	Audit Review, Analysis, and Reporting | Integration / Scanning and Monitoring Capabilities
AU-6(6)	Audit Review, Analysis, and Reporting | Correlation With Physical Monitoring
CA-3	System Interconnections
CA-3(5)	System Interconnections | Restrictions on External Network Connections
CA-9	Internal System Connections

ID	Title
CM-11	User-Installed Software
CM-11(1)	User-Installed Software | Alerts For Unauthorized Installations
CM-11(2)	User-Installed Software | Prohibit Installation without Privileged Status
CM-2	Baseline Configuration
CM-3	Configuration Change Control
CM-3(2)	Configuration Change Control | Test / Validate / Document Changes
CM-3(6)	Configuration Change Control | Cryptography Management
CM-4	Security Impact Analysis
CM-4(1)	Security Impact Analysis | Separate Test Environments
CM-5	Access Restrictions For Change
CM-5(1)	Access Restrictions For Change | Automated Access Enforcement / Auditing
CM-5(2)	Access Restrictions For Change | Review System Changes
CM-5(5)	Access Restrictions For Change | Limit Production / Operational Privileges
CM-5(6)	Access Restrictions For Change | Limit Library Privileges
CM-6	Configuration Settings
CM-6(2)	Configuration Settings | Respond to Unauthorized Changes
CM-7	Least Functionality
CM-7(1)	Least Functionality | Periodic Review
CM-7(3)	Least Functionality | Registration Compliance
CM-8	Information System Component Inventory
CM-8(1)	Information System Component Inventory | Updates During Installations / Removals
CM-8(3)	Information System Component Inventory | Automated Unauthorized Component Detection
CM-9	Configuration Management Plan
CP-10	Information System Recovery and Reconstitution
CP-2	Contingency Plan
CP-2(1)	Contingency Plan | Coordinate With Related Plans
CP-2(3)	Contingency Plan | Resume Essential Missions / Business Functions
CP-2(4)	Contingency Plan | Resume All Missions / Business Functions
CP-7	Alternate Processing Site
CP-7(1)	Alternate Processing Site | Separation From Primary Site
CP-7(2)	Alternate Processing Site | Accessibility
CP-7(3)	Alternate Processing Site | Priority of Service
CP-7(4)	Alternate Processing Site | Preparation for Use
CP-8	Telecommunications Services
CP-8(1)	Telecommunications Services | Priority of Service Provisions
CP-8(2)	Telecommunications Services | Single Points of Failure
CP-8(3)	Telecommunications Services | Separation of Primary / Alternate Providers
CP-8(4)	Telecommunications Services | Provider Contingency Plan
IA-2	Identification and Authentication (Organizational Users)
IA-2(2)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts

ID	Title
IA-2(8)	Identification and Authentication (Organizational Users) | Network Access to Privileged Accounts - Replay Resistant
IA-2(9)	Identification and Authentication (Organizational Users) | Network Access to Non-Privileged Accounts - Replay Resistant
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication
IA-4	Identifier Management
IA-4(4)	Identifier Management | Identify User Status
IA-5	Authenticator Management
IA-5(1)	Authenticator Management | Password-Based Authentication
IA-5(13)	Authenticator Management | Expiration of Cached Authenticators
IA-5(3)	Authenticator Management | In Person or Trusted Third-Party Registration
IA-5(4)	Authenticator Management | Automated Support for Password Strength Determination
IR-8	Incident Response Plan
MA-2	Controlled Maintenance
MA-3(2)	Maintenance Tools | Inspect Media
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal
MA-5(1)	Maintenance Personnel | Individuals Without Appropriate Access
MP-2	Media Access
MP-3	Media Marking
MP-4	Media Storage
MP-5	Media Transport
MP-5(4)	Media Transport | Cryptographic Protection
MP-6	Media Sanitization
MP-7	Media Use
MP-7(1)	Media Use | Prohibit Use without Owner
PE-11	Emergency Power
PE-11(1)	Emergency Power | Long-Term Alternate Power Supply - Minimal Operational Capability
PE-13	Fire Protection
PE-14	Temperature and Humidity Controls
PE-15	Water Damage Protection
PE-15(1)	Water Damage Protection | Automation Support
PE-2	Physical Access Authorizations
PE-3	Physical Access Control
PE-3(1)	Physical Access Control | Information System Access
PE-4	Access Control For Transmission Medium
PE-6	Monitoring Physical Access
PE-6(1)	Monitoring Physical Access | Intrusion Alarms / Surveillance Equipment
PE-6(4)	Monitoring Physical Access | Monitoring Physical Access to Information Systems
PE-9	Power Equipment and Cabling
PS-2	Position Risk Designation
PS-3	Personnel Screening
PS-4	Personnel Termination

ID	Title
PS-5	Personnel Transfer
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
RA-5	Vulnerability Scanning
SC-10	Network Disconnect
SC-12	Cryptographic Key Establishment and Management
SC-15	Collaborative Computing Devices
SC-18	Mobile Code
SC-18(1)	Mobile Code | Identify Unacceptable Code / Take Corrective Actions
SC-18(2)	Mobile Code | Acquisition / Development / Use
SC-18(3)	Mobile Code | Prevent Downloading / Execution
SC-18(4)	Mobile Code | Prevent Automatic Execution
SC-23(1)	Session Authenticity | Invalidate Session Identifiers At Logout
SC-23(3)	Session Authenticity | Unique Session Identifiers With Randomization
SC-24	Fail In Known State
SC-28	Protection of Information At Rest
SC-28(1)	Protection of Information At Rest | Cryptographic Protection
SC-38	Operations Security
SC-5	Denial of Service Protection
SC-5(1)	Denial of Service Protection | Restrict Internal Users
SC-5(2)	Denial of Service Protection | Excess Capacity / Bandwidth / Redundancy
SC-5(3)	Denial of Service Protection | Detection / Monitoring
SC-7	Boundary Protection
SC-7(10)	Boundary Protection | Prevent Unauthorized Exfiltration
SC-7(11)	Boundary Protection | Restrict Incoming Communications Traffic
SC-7(12)	Boundary Protection | Host-Based Protection
SC-7(13)	Boundary Protection | Isolation of Security Tools / Mechanisms / Support Components
SC-7(14)	Boundary Protection | Protect Against Unauthorized Physical Connections
SC-7(18)	Boundary Protection | Fail Secure
SC-7(21)	Boundary Protection | Isolation of Information System Components
SC-7(3)	Boundary Protection | Access Points
SC-7(4)	Boundary Protection | External Telecommunications Services
SC-7(9)	Boundary Protection | Restrict Threatening Outgoing Communications Traffic
SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
SC-8(2)	Transmission Confidentiality and Integrity | Pre / Post Transmission Handling
SI-10	Information Input Validation
SI-10(3)	Information Input Validation | Predictable Behavior
SI-10(4)	Information Input Validation | Review / Timing Interactions

ID	Title
SI-16	Memory Protection
SI-2	Flaw Remediation
SI-2(1)	Flaw Remediation | Central Management
SI-2(2)	Flaw Remediation | Automated Flaw Remediation Status
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-4(1)	Information System Monitoring | System- Wide Intrusion Detection System
SI-4(10)	Information System Monitoring | Visibility of Encrypted Communications
SI-4(11)	Information System Monitoring | Analyze Communications Traffic Anomalies
SI-4(12)	Information System Monitoring | Automated Alerts
SI-4(19)	Information System Monitoring | Individuals Posing Greater Risk
SI-4(2)	Information System Monitoring | Automated Tools For Real-Time Analysis
SI-4(22)	Information System Monitoring | Unauthorized Network Services
SI-4(23)	Information System Monitoring | Host-Based Devices
SI-4(4)	Information System Monitoring | Inbound and Outbound Communications Traffic
SI-4(5)	Information System Monitoring | System- Generated Alerts
SI-5	Security Alerts, Advisories, and Directives
SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks
SI-7(14)	Software, Firmware, and Information Integrity | Binary or Machine Executable Code
SI-7(8)	Software, Firmware, and Information Integrity | Auditing Capability For Significant Events

Appendix E: ISSO RESPONSIBILITIES

Maintain Professional certification as outlined in DoD 8570.01-M.
Ensure Cyber and Cyber-enabled software, hardware, and firmware comply with appropriate security configuration guidelines.
Ensure C2BMC recovery processes are monitored and that Cyber features and procedures are properly restored.
Report all Critical Information Requirements to include all non-compliances with DoD C&A / A&A Packages, all configuration changes executed without ISSM approval, and ensure that all users fulfill their Cyber obligations as required by ISSM and enforced by ISSO.
Ensure scanning and auditing on all C2BMC is performed IAW published guidance.
Implementing and enforcing all Cyber policies and procedures, as defined by the C2BMC security documentation both in DIACAP and Risk Management Framework, as appropriate and determined by the ISSM.
On behalf of the ISSM and in collaboration with the C2BMC Control Center (CCC) and MDA CERT (as appropriate) validate and coordinate all Cyber related task orders.
On behalf of the ISSM and in collaboration with the CCC, JFCC-IMD, and MDA CERT, initiate and direct, as applicable, the appropriate protective or corrective measures when a Cyber incident, event or vulnerability is discovered.
Assist the ISSM in coordinating and monitoring Cyber connection approvals applicable to the C2BMC sites (SIPRNET, DATMS-U, MSPP, Cross Domain Solutions, etc.).
Assist the ISSM in coordinating support for Cyber Staff Assistance Visits, MDA Control Validation Test teams, National Security Agency Red and Blue Teams, Defense Information Systems Agency Command Cyber Readiness Inspections and other inspection/compliance teams as required.
Ensure that all C2BMC system users, to include privileged users, on the program have satisfied their initial, recurring, and Privileged User Cyber training in accordance with governing directives.
Ensure that all C2BMC users have signed a User Agreement form and it is on file.
Ensure that all privileged C2BMC users have signed User Agreement and Privileged User Agreement forms, and that those forms are kept on file. Ensure all users are effectively removed from systems in a timely manner when access is no longer required.
Ensure personnel who perform work in positions identified as both Cyber Management and Technical levels obtain the requisite technical level certifications, as required by BC.