C2BMC Spiral Capability Development Contract

C2BMC Operations & Maintenance, Logistics, & CCMD Integration

Task Order 7002

Rev 1

April 6, 2018

Table of Contents

1.0 Background 4

2.0 Technical Expert Status Accreditation (TESA) 4

3.0 Program Management 4

3.1 Integrated Process and Product Development (IPPD) 5

3.2 Contractor Integrated Performance Management 5

3.3 Integrated Baseline Reviews (IBRs) 5

3.4 Process Control 5

3.5 Program Reviews 5

3.6 Bills of Material Management (BOM) 6

3.7 Software Data Reporting 6

3.8 Quality, Safety and Mission Assurance Management 6

4.0 Operations & Maintenance 6

4.1 Level I On-Site Operations & Maintenance: 6

4.2 C2BMC Command Center: 7

4.3 Level II Maintenance (Help Desk): 7

4.4 Information System Security Officers (ISSOs): 7

5.0 Integrated Logistics Support: 8

5.1 Logistics Support 8

5.2 Supply Chain Management: 8

5.3 Sustaining Engineering 9

5.3.1 Reliability, Availability, and Maintainability (RAM): 9

5.3.2 Obsolescence Engineering: 9

5.3.3 Cybersecurity: 9

5.3.4 Warfighter Requirements: 10

5.3.5 Continuous Improvement Program (CIP): 10

5.3.6 External/Internal System Configuration Changes: 10

5.3.7 Level III Maintenance (SME Reach Back): 10

5.4 Software Modification Requests (SMRs)/Troubleshooting Procedures (TPs 10

5.5 Decommissioning and Retrograde of Equipment 10

6.0 Risk Management Framework: 11

6.1 RMF Authorization Maintenance: 11

6.2 RMF Plan of Action and Milestones (POAMs): 11

7.0 CCMD Integration: 12
7.1 Liaison Officers (LNOs): 12
7.2 Training Delivery: 12
7.3 Subject Matter Experts: 12
7.4 Demonstrations, RFIs/RFAs, Assessment Activities, Real World Events/ Contingency Operations 13
8.0 Major Deployments, Minor Deployment, and System Configuration Changes: 14
8.1 System Configuration Changes: 14
8.1.1 IA Patches: 14
8.2 Minor Deployment: 14
8.2.1 C2BMC Common Operating Picture (COP): 15
8.2.2 Position Navigation & Timing (PNT) Integration: 15
8.2.3 Add BMDS C2BMC Modes (BCM) to DTS Node: 15
8.2.4 Camp Roberts Move: 15
8.3 Major Deployments: 15
8.3.1 USFK User Node: 15
8.4 Defense Red Switch Network (DRSN): 15
9.0 Period of Performance 16
10.0 Task Order Monitor 16
11.0 Travel 16
12.0 Deliverables 16
13.0 Government Furnished and Contractor Acquired Property 16
14.0 Places of Performance 16
15.0 Acronym List 17

1.0 Background

This Task Order (TO) provides Operations & Maintenance, Integrated Logistics, Combatant Command (CCMD) Integration, Deployment, and Disposal of the Command and Control, Battle Management and Communications (C2BMC) deployed systems. This effort is a follow-on and continuation of the Sustainment and Warfighter Integration effort provided under HQ0147-12-D-0003, Task Order 13 – C2BMC Spiral 6.4 Operations & Maintenance, Logistics, Warfighter Integration, and Deployment.

2.0 Technical Expert Status Accreditation (TESA)

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

2.1 For Contractor personnel serving in an Area of Responsibility (AOR) that requires TESA and in accordance with (IAW) the current version of Department of Defense Instruction (DoDI) 3020.37, "Continuation of Essential DoD Contractor Services During Crisis", overseas positions supporting the Contingency Architecture Activation Team effort in (b)(3):10 U.S.C. § 130 and other overseas positions supporting MDA under this Contract, the Contracting Officer hereby designates the following positions/job functions as Emergency/Mission Essential:

a. United States European Command (EUCOM) Operations and Sustainment (O&S) Lead/Technical Expert (TE)
b. Architecture and System Engineering (A&SE) CCMD 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. Warfighter 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 IAW 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, executing, monitoring, reporting, and managing for this Task Order (TO).

The Contractor shall establish a Failure Review Board (FRB), to determine root cause and requires 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 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), 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 Software Data Reporting

The Contractor shall systematically collect and report actual contract costs and metrics (CDRL A149) to provide DoD cost analysts with needed data to estimate future costs. Software Resources Data Reports shall be prepared IAW the instructions contained in the most recently approved version of DI-MGMT-82035.

IAW DODI 5000.02 and DFARS 252.234-7003, Notice of Cost and Software Reporting System, the Contractor shall use a documented standard cost and software data reporting (CSDR) process that satisfies the guidelines contained in the DoD 5000.04–M–1, CSDR Manual. The contractor shall use the Government-approved CSDR plan for this contract, DD Form 2794, updated to reflect the most current task orders, and the related Resource Distribution Table as the basis for reporting IAW the required CSDR data item descriptions (DIDs).

The Contractor shall report SRDR maintenance reporting on all programs previously qualified for SRDR development reporting or currently qualified for CCDR sustainment reporting (i.e., total contract exceeding $50M, then year dollars), where the total current annual software maintenance effort exceeds $1M per year, then year dollars

3.8 Quality, Safety and Mission Assurance Management

IAW 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 Appendices A-6/A-8, the staffing & response times in Appendices A-6/A-8 to the C2BMC system demarcation (demarc) in Appendix F, 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 Appendices A-6/A-

8 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 PACOM Pearl Harbor site listed in Appendix A-6, adhering to local Joint Base Pearl Harbor Hickam physical security standards until decommission at site is complete.

4.2 C2BMC Command Center:

The Contractor shall provide a C2BMC Command 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 Appendices A-6/A-8 to the demarc point in Appendix F.

The Contractor shall provide Local Control Center (LCC) (Tier 3 Computer Network Defense support Cybersecurity Computer Network Defense Service Provider support to the MDA Computer Emergency Response Team (CERT) Tier 2 (CNDSSP) for continuous active monitoring of the security posture of the Contractor sites and systems connected to MDA CNet architecture.

The Contractor shall coordinate with Cyber Protection Teams, MDA Computer Network Defense Service Provider (CNDSP) / 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 meet requirements for the comprehensive security of C2BMC.

4.3 Level II Maintenance (Help Desk):

The CCC shall provide Level II maintenance and help desk support for all C2BMC operational, test, and training equipment at sites identified in Appendices A-6/A-8 up to demarc point in Appendix F.

4.4 Information System Security Officers (ISSOs):

The Contractor shall fulfill the duties and responsibilities of an ISSO IAW the current DoDI 8500.01 Cybersecurity, 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. 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.

The Contractor shall provide the C2BMC ISSM a copy of the most recent DSS/DAA authorization documentation. The Contractor shall formally report to the ISSM, AO, and other affected parties any cybersecurity-related or configuration changes that may impact the C2BMC program. The Contractor shall formally report to the ISSM of any site cybersecurity inspections, tests, and reviews that are taking place on C2BMC authorized Information Systems (IS). The Contractor shall follow cyber incident reporting guidance per the DoD Federal Acquisition Regulations 252.204-7012.

The Contractor shall provide inputs to and support Government security analyses, including system security analyses, the System Vulnerability Analysis (SVA), Operations Security (OPSEC) Planning, System Security Engineering (SSE) requirements analysis, and Information Assurance (IA)/Computer Network Defense (IA/CND) technical assessments.

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 and other equipment identified in Appendices A-6/A-8 up to the demarc in Appendix F. The Contractor shall provide integrated logistics support to C2BMC operational, test, and training systems at all locations IAW Appendices A-6/A-8, the staffing & response times in Appendices A-6/A-8, and to the availability levels specified in the MDA System Specification (Classified). The Contractor shall maintain support and availability to the system 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 Appendices A-6/A-8 up to the demarc point in Appendix F, the staffing & response times in Appendices A-6/A-8, and to the availability levels specified in the MDA System Specification (Classified). The Contractor shall coordinate when providing O&S/Supply Chain actions for all Government Property not included on HQ0147-12-D-0003, Attachment 9. The Contractor shall maintain a logistics management information system. The Contractor shall provide hardware and software supply chain security IAW MDA Parts, Materials, and Processes Mission Assurance Plan (PMAP), MDA Policy Memorandum 50, and paragraph 6.3.1 of the base IDIQ contract.

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 Appendices A-6/A-8 up to the demarc point in Appendix F 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 Failure Reporting, Analysis, and Corrective Action System 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 Appendices A-6/A-8 up to the demarc point in Appendix F 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:

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 deployed spirals. The Contractor shall recommend cybersecurity architecture strategy changes for government approval and will include C2BMC Command Center (CCC) in the architecture. 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 Appendices A-6/A-8 up to the demarc in Appendix F. 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.

5.3.4 Warfighter Requirements:

The Contractor shall perform engineering and analysis of Warfighter feedback and Warfighter Improvement Process WIP submittals selected by the Government 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 SMR process for prioritization and development.

5.3.5 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 SMR process, but instead will focus on support tool, process, and quality of life improvements.

5.3.6 External/Internal System Configuration Changes:

The Contractor shall perform engineering analysis for externally driven interface and/or configuration changes for C2BMC systems listed in Appendices A-6/A-8 up to demarc point in Appendix F to include GFX Government Cybersecurity 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 SMR process for prioritization and development. The Contractor shall update and maintain Government required cyber toolsets.

5.3.7 Level III Maintenance (SME Reach Back):

The Contractor shall provide scheduled and/or unscheduled off-site maintenance SME reach back support for equipment in Appendices A-6/A-8 up to demarc point in Appendix F 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 and Planner Software.

5.4 Software Modification Requests (SMRs)/Troubleshooting Procedures (TPs

The Contractor shall develop and test SMRs/TPs for all C2BMC ops, planning, test, and training systems 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. The Contractor shall update all engineering artifacts and associated documentation as required.

5.5 Decommissioning and Retrograde of Equipment

The Contractor shall decommission and retrograde Spiral 6.4 equipment in Appendix A-6 in the PACOM region only IAW DFARS 252.245-7004 and established decommissioning plans, including actions required for restocking of equipment as spares and departure from dedicated Spiral 6.4 facilities.

6.0 Risk Management Framework:

The Contractor shall plan, conduct, and manage the C2BMC RMF IAW Appendix B and Government templates (CDRL A095, A124). The Contractor shall initiate and/or maintain RMF package(s), ATOs, and ATCs for C2BMC systems in appendices A-6/A-8 to the demarc point in Appendix F IAW Cybersecurity Guidance Documents in Appendix B and C2BMC Program Protection Plan (CDRL A095, 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.

6.1 RMF Authorization Maintenance:

The Contractor shall support and maintain C2BMC program SIPRNet connection to include maintaining a Web-based data repository, controlling access to the Web site and facilitating Memorandum of Agreement(s) (MOA[s]) discussions for access to external SIPRNet sites. The Contractor shall obtain and maintain authorizations and connection approvals necessary to sustain C2BMC operations, training/exercises, and testing for systems in Appendices A-6/A-8 up to the demarc in Appendix F. 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, Very High, and High RMF findings within 30 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all CAT II and Moderate RMF findings within 90 days. The Contractor shall correct, mitigate, or submit risk acceptance package of all CAT III, Low, and Very Low RMF findings within 180 days. The Contractor shall update existing packages in eMASS, as required, until transition to RMF packages in eMASS are complete to eliminate any lapses in cybersecurity authorizations.

6.2 RMF Plan of Action and Milestones (POAMs):

The Contractor shall conduct and upload a monthly vulnerability auto-scan database as designated by the Government and evaluate within 30 days. The Contractor shall develop Plan of Action and Milestones (POA&M) IAW Appendix B and Government templates and time lines for systems in Appendices A-6/A-8 up to the demarc in Appendix F. 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 database, 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).

7.0 CCMD Integration:

7.1 Liaison Officers (LNOs):

The Contractor shall fulfill LNO responsibilities for all C2BMC COCOM locations and in support of HQ MDA Ft. Belvoir/NMCC and MDA Huntsville. The Contractor LNO shall maintain up-to-date knowledge and documentation of CCMD-specific doctrine, plans, C2 structure and C2 execution, TTPs, etc., as it pertains to the use and contribution of C2BMC operations to that CCMD's Area of Responsibility (AOR). The Contractor shall require all LNO's maintain C2BMC SME status. The Contractor LNO shall update and brief CCMD HQ staff on all C2BMC system and SME involvement in wargames, exercises, test events, and operational events. The Contractor LNO shall provide information briefings and education support to staff in their respective AORs and, upon program office direction, be able to support meetings in theater to provide technical expertise at such events as exercise planning, TTP development, BMD planning, and other senior leader engagements where C2BMC technical support is warranted.

7.2 Training Delivery:

The Contractor shall support 19 Wargames, Exercises, and Table Top Exercises (TTXs), from 1 July 2018 (conclusion of TO15) – 15 November 2019 where C2BMC is emulated, to include Mobile Training Team (MTT) support as required, IAW C2BMC Test Baseline, IMTP, and Integrated Master Wargames and Exercises Plan (IMWEP). The Contractor shall participate in Planning Conferences, Scenario Design Working Groups, and other exercise related Working Groups with C2BMC objectives and/or C2BMC emulation as directed by the Government. The Contractor shall assess proposed architectures for suitability of event objectives and provide the Government Courses of Actions (COAs) for each event to the C2BMC System Test Integration Board (CSTIB). The Contractor shall supply information to the MDA/BC Government Lead in support of an Event Sheet briefing for all Wargames and Exercises to be presented at the C2BMC Event Status Review and producing a Final Report to close out all discoveries and Lessons Learned from the event. The Contractor shall provide analysis for Wargames, Exercises, and TTXs as directed by the Government. The Contractor shall provide a concise schedule of support to include personnel management for planning conferences, integration and execution periods and projected travel requirements. The Contractor shall provide and maintain training material, provide a combined total of 20 classes for S6.4 training) to operators and SMEs, and S8.2 training to SMEs. The Contractor shall troubleshoot, modify, and/or develop training scenarios.

7.3 Subject Matter Experts:

The Contractor shall maintain the C2BMC SME Program. The objective of the C2BMC SME program is to provide a qualified pool of operationally knowledgeable individuals who can offer technical advice to developers, provide overview briefings to senior leaders, and perform over-the-shoulder support to warfighters during the operation and fielding of new spirals of the C2BMC program. Each SME shall be well versed in the technical underpinnings of C2BMC operations to include system behavior and linkages to other parts of the BMDS. In addition to understanding the technical details of C2BMC, each SME shall be familiar with each CCMD's operational BMD structure (organization and assets) and overall BMDS concept of employment. The contractor shall develop a plan to identify, train,

certify and schedule SMEs to support high visibility events as directed by the government. As noted in paragraph7.1, LNOs shall be qualified under the C2BMC SME program.

In addition to Operational C2BMC SMEs, the Contractor shall establish a Planner Support Cell (PSC) to provide tailored C2BMC Planner and SME support to the Warfighter and test community. The PSC shall provide defense design briefs and participate in working groups as directed by the Government. PSC support shall include analysis and modification for current defense designs, test plan development, defense design analysis and experimentation as directed. All Contractor SMEs shall support development, modification and loading of operational, test, exercise, and training defense designs for all fielded C2BMC baselines. The PSC shall provide planner SME and technical support for operational Planner locations and program office support in Huntsville & MDIOC.

7.4 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 A&A, Cyber Protection Team (CPT), Color Team (e.g. Red/Blue/Green), ECRE, and CCMD 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.

Upon Government request, the Contractor shall provide C2BMC SMEs at locations participating in any exercises, test events, wargames, training events, or targets of opportunities/real world events where additional SME support may be required. The Contractor SMEs shall be cognizant of all C2BMC functionalities performed during the event and submit inputs for all requested information upon event completion. The Contractor shall seek the government's approval for initial establishment and any modification to the C2BMC SME program.

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.

The Contractor shall deliver results to the Government IAW Task Instruction(s) in Attachment 8.

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

For each major deployment, minor deployment, and all system configuration changes, the Contractor shall provide an appropriate test approach 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 approach, the contractor shall assist in the EOW so that assets and BMDS elements can be scheduled. The Contractor shall present the test approach 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, A124). 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.

8.1 System Configuration Changes:

The Contractor shall install and test configuration changes, approved by the Program Engineering Review Board (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.

8.1.1 IA Patches:

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 A055). The Contractor shall provide IA releases to the S8.2 C2BMC architecture on a quarterly basis (only in an emergency for S6.4 C2BMC architecture) 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.

8.2 Minor Deployment:

The Contractor shall deploy minor deployments, approved by the PERB, ICCB, TCMB, ISG, and/or PCB. The contractor shall keep test and training system configurations consistent with operational system configurations.

8.2.1 C2BMC Common Operating Picture (COP):

The Contractor shall engineer and integrate the C2BMC Common Operating Picture (COP) capability into a lab environment.

8.2.2 Position Navigation & Timing (PNT) Integration:

The Contractor shall integrate C2BMC systems with the new Government furnished GPS/PNT systems installed at C2BMC locations as these new systems become available.

8.2.3 Add BMDS C2BMC Modes (BCM) to DTS Node:

The Contractor shall add Cybersecurity compliant BCM to DTS Node to support CCMD exercise integration.

(b)(3):10 U.S.C. § 130

8.2.4 [redacted] Move:

(b)(3):10 U.S.C. § 130

The Contractor shall procure, install, integrate and operationalize a new [redacted] BMDS Teleport Gateway (BTG) hardware and communication links, thereby moving the operational capability from its current location in the SATCOM operations building, Bldg

(b)(3):10 U.S.C. § 130

[redacted] to the new Satellite Earth Terminal Station (SETS) building, Bldg [redacted]. Upon successful testing and operationalization, the Contractor shall decommission the BTG in Bldg [redacted]

(b)(3):10 U.S.C. § 130

(b)(3):10 U.S.C. § 130

8.2.5 BTG Safety Upgrade:

The Contractor shall provide BTG safety upgrades in CENTCOM.

8.3 Major Deployments:

The Contractor shall deploy major deployments, approved by the PERB, ICCB, TCMB, ISG, and/or PCB. The contractor shall keep test and training system configurations consistent with operational system configurations.

(b)(3):10 U.S.C. § 130

8.3.1 [redacted] User Node:

The Contractor shall assemble user node equipment in the lab and complete initial testing. Once complete, the Contractor shall disassemble, pack, ship, install, Cycle 5 test and operationalize the [redacted] User Node at the deployed location.

(b)(3):10 U.S.C. § 130

8.4 Defense Red Switch Network (DRSN):

The Contractor shall provide installation, integration, and testing services to support MDA in the development, implementation and fielding of Secure Voice subsystems across the Department of Defense community. The Contractor shall support the reconfiguration of infrastructure and activation of MDA circuits to and from locations. The Contractor shall support the installation and activation of new DRSN circuits for test locations and hosting Red Switch locations. The Contractor shall provide cabling and hardware as required to

support circuits. The Contractor shall provide personnel with a secret clearance and secure and non-secure DRSN certificate of training. Personnel must be familiar with the functionality of DRSN assets to minimize downtime to the customer and capable of upgrading DRSN assets to the latest version firmware. The Contractor shall provide DRSN design configuration test support and Red Switch to remote site mockups. The Contractor shall reconfigure and test service to switches and provide as-built drawings via the DAL. The Contractor shall support Technical Interchange Meetings (TIMs).

9.0 Period of Performance

16 December 2017 through 15 November 2019.

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
A052	Preliminary System Security Concept
A055	Patch Management Plan
A095	PPS Registration
A124	System Security Plan
A149	Software Resources Data Report

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. Government Furnished Property (GFP) is furnished in an “as is” condition in accordance with FAR 52.245-1.

.

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
ADSI	Active Directory Service Interface
AO	Authorizing Official
BCN	BMDS Communications Network
BMD	Ballistic Missile Defense
BMDS	Ballistic Missile Defense System
BNOSC	BMDS Network Operations and Security Center
BOA	BMDS OPIR Architecture
BOM	Bills of Material
BORRS	BMDS Operational Readiness Reporting System
C2	Command and Control
C2BMC	Command and Control, Battle Management and Communications
COA	Course of Action
CCC	C2BMC Command Center
CCMD	Combatant Command
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
COMSEC	Communications Security
CONOPS	Concepts of Operations
CONUS	Continental United States
COOP	Continuity of Operations Procedures
COP	Common Operating Picture
CPT	Cyber Protection Team
CSSC	C2BMC System Support Center
CSTIB	C2BMC System Test Integration Board
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
DRSN	Defense Red Switch Network
DSB	Data Scoring Board
DTS	Distributed Training System
DUC	Downloadable Unified Client

EIE	Element Interface Equipment
eMASS	Enterprise Mission Assurance Support 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
HNI	Host Nation Interface
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

ORR	Operational Readiness Review
OTA	Operational Test Agency
PACOM	Pacific Command
PCB	Program Change Board
PCO	Procurement Contracting Officer
PERB	Program Engineering Review Board
PMIs	Preventative Maintenance Inspections
PMO	Project Management Office
PNT	Position Navigation & Timing
POC	Point of Contact
PPS	Ports, Protocols, and Services
PSC	Planner Support Cell
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
SRDR	Software Resources Data Report
SOW	Statement of Work
STOC	System Test and Operations Center
STRATCOM - OFFUTT	Strategic Command - Offutt Air Force Base
TO	Task Order
TCMB	Training Configuration Management Board
TE	Technical Expert
TESA	Technical Expert Status Accreditation
TO	Task Order
TP	Troubleshooting Procedure
TSS	Training System Sustainment
TTPs	Test, Training, and Procedures
USFK	United States Forces Korea
VAFB	Vandenberg Air Force Base
WF	Warfighter

Appendix A-6: Spiral 6.4 C2BMC Equipment Locations and Responsibilities

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1			No
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1 & Security, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2, 3			
			1, 2, 3			Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2			
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1,2,3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1,2,3			Yes
			1, 2, 3			Yes
			1			No
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1 w/ DISA, 2, 3			Yes
			1 w/ DISA, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1 w/DISA, 2, 3			Yes
			2, 3			Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			1 w/ DISA, 2, 3			Yes
			1			No, GFX
			1 w/ DISA, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2			No
			1, 2, 3			Yes
			1, 2, 3 for Hardware			Yes, Hardware
			Key only			No
			1, 2, 3			HW Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			No
			1* (Campus Comms)			No
(b)(3):10 U.S.C. § 130;(b)(7)(E)						

Appendix A-8: Spiral 8.2 C2BMC Equipment Locations and Responsibilities

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)				(b)(3):10 U.S.C. § 130;(b)(7)(E)		
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2,			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2			No
			1, 2, 3			Yes
			1, 2, 3			(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		(b)(3):10 U.S.C. § 130;(b)(7)(E)
			1*, 2			No, PM-WESS (b)(3):10 U.S.C. §
			1*, 2, 3 (*via			Yes (b)(3):10 U.S.C. §
			1, 2			No
			(b)(3):10 U.S.C. § 130;(b)(7)(E)			Yes
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1*, 2, 3			Yes
			1*, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1 , 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			1, 2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			2, 3			Yes
			1, 2, 3			Yes

AOR	Location	System	O&M Levels (SOW 4.1, 4.3, 5.3.7)	Duty Shift	Recall Time	ILS/Sustain (SOW 5.0)
(b)(3):10 U.S.C. § 130;(b)(7)(E)			1, 2, 3	(b)(3):10 U.S.C. § 130;(b)(7)(E)		Yes
			1, 2			No
			1, 2, 3			Yes
			1, 2, 3 for Hardware			Yes, Hardware
			(b)(3):10 U.S.C. § 130;(b)(7)(E)			No
			1, 2, 3			Yes
			1, 2, 3			Yes
			2, 3			Yes
			2, 3			No
			(b)(3):10 U.S.C. § 130;(b)(7)(E)			No

(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	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-	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: 6.4 ISSO Locations

S6.4 ISSO Support		
(b)(3):10 U.S.C. § 130;(b)(7)(E)	On Site	Off Site
	X	
	X	
		X
	X	
		X
	X	
		X
	X	
	X	
		X
		X
		X
	X	X

Appendix D: 8.2 ISSO Locations

S8.2 ISSO Support		
(b)(3):10 U.S.C. § 130;(b)(7)(E)	On Site	Off Site
	X	
	X	
	X	
		X
	X	
	X	
	X	
	X	
		X
	X	

Appendix E: ISSO RESPONSIBILITIES

Maintain Professional certification as outlined in DoD 8570.01-M.
Enforce security configuration guidelines compliance with all Cyber and Cyber-enabled software, hardware, and firmware.
Monitor C2BMC recovery processes and properly restore Cyber features and procedures.
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 require that all users fulfill their Cyber obligations as required by ISSM and enforced by ISSO.
Perform scanning and auditing on all C2BMC IAW published guidance.
Implement and enforce all Cyber policies and procedures, as defined by the C2BMC security documentation in Risk Management Framework, as appropriate and determined by the ISSM.
On behalf of the ISSM and in collaboration with the (b)(3):10 U.S.C. § 130;(b)(7)(E) MDA CERT (as appropriate) validate and coordinate all Cyber related task orders.
On behalf of the ISSM and in collaboration with the (b)(3):10 U.S.C. § 130;(b)(7)(E) and MDA CERT, initiate and direct 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.
Require all C2BMC system users, to include privileged users, on the program have satisfied their initial, recurring, and Privileged User Cyber training IAW governing directives.
Require all C2BMC users to sign a User Agreement form and keep it on file.
Require all privileged C2BMC users have signed User Agreement and Privileged User Agreement forms, and keep those forms on file. When access is no longer required, remove all users from systems in a timely manner.
Require personnel who perform work in positions identified as both Cyber Management and Technical levels obtain the requisite technical level certifications, as required by BC.

APPENDIX F: O&M Demarcation Points

AOR	Location	Demarcation Point
(b)(3):10 U.S.C. § 130;(b)(7)(E)		