



**C2BMC Spiral Capability Development Contract**

**Spiral 8.2 Statement of Work**

**March 27, 2017**

**Final**

**Modification P00064**

## Table of Contents

1.0	SCOPE .....	8
1.1	General.....	8
1.2	Specific Terms and Definitions .....	8
1.3	C2BMC Element.....	8
2.0	APPLICABLE DOCUMENTS .....	<b>Error! Bookmark not defined.</b>
2.1	Compliance Documents .....	<b>Error! Bookmark not defined.</b>
2.2	Guidance Documents .....	<b>Error! Bookmark not defined.</b>
2.2.1	Department of Defense Documents .....	<b>Error! Bookmark not defined.</b>
2.2.2	Missile Defense Agency (MDA) Documents .....	<b>Error! Bookmark not defined.</b>
2.2.3	Other Government Documents .....	<b>Error! Bookmark not defined.</b>
2.3	Contractor Documents & Industry Standards, Specifications, and References.....	13
3.0	PROGRAM MANAGEMENT.....	13
3.1	Integrated Process and Product Development (IPPD).....	14
3.2	Contractor Integrated Performance Management.....	14
3.3	Integrated Baseline Reviews (IBRs).....	14
3.4	Integrated Master Schedule (IMS).....	14
3.5	Process Control .....	14
3.6	Program Reviews .....	14
3.7	Subcontract Management.....	15
3.8	Contract Work Breakdown Structure (CWBS).....	15
3.9	Contract Performance Report (CPR) .....	15
3.10	Contract Funds Status Report (CFSR).....	15
3.11	Cost Working Group (CWG).....	15
3.12	Cost Analysis Requirements Description .....	15
3.13	Cost and Software Data Reporting (CSDR) .....	15
3.13.1	Cost Data Reporting.....	15
3.13.2	Software Data Reporting.....	15
3.14	Risk and Opportunity Management .....	15
3.15	Searchable Repository .....	16
3.15.1	Program Data .....	19
3.15.2	Data Access.....	19
3.15.2.1	<b>Unclassified Repository .....</b>	<b>19</b>
3.15.2.2	<b>Classified Repository .....</b>	<b>20</b>
3.16	Data Accession List .....	20
3.17	Information Initiatives .....	20
3.18	Rough Order of Magnitude (ROM) .....	20
4.0	SYSTEMS ENGINEERING .....	20
4.1	C2BMC Architecture .....	21
4.2	C2BMC Build Specifications (CBS) .....	21
4.3	C2BMC Spiral Specifications (CSS).....	21
4.3.1	Integrated Engineering.....	21
4.3.2	System/Software Engineering.....	22
4.3.3	Part 1 and Part 2 Interface Control Document (ICD) Support.....	22
4.3.4	User Interface Engineering .....	22

4.3.5	High-Altitude Electromagnetic Pulse (HEMP), Electrostatic Discharge (EDS), ENVIRONMENTAL .....	23
4.4	Department of Defense (DoD) Information Technology Standards Registry (DISR) .	23
4.5	Dynamic Object-Oriented Requirements System (DOORS).....	23
4.6	Analysis and Assessments .....	23
4.6.1	Analysis Report.....	23
4.7	Technical Performance Measurement (TPM).....	23
4.8	Program Report Database (PRD).....	24
4.9	System Engineering Management Plan (SEMP) .....	24
4.10	System Integration Assessments and Special Studies .....	24
4.11	Engineering Verification and Validation .....	24
4.11.1	Spiral Capability Verification Plan (SCVP) .....	24
4.11.2	Spiral Capability Assessment Report (SCAR) .....	24
4.12	C2BMC Modeling and Simulation (M&S).....	24
4.13	C2BMC Algorithm Engineering.....	25
4.13.1	C2BMC Algorithm Documentation, Reference Implementation, and Software ....	25
4.14	Element Effectiveness Performance Assessment .....	25
4.15	C2BMC Element Interoperability.....	26
4.16	Labs, Models, Simulations, and Testbeds Maintenance .....	26
4.16.1.1	<b>Testing Activities at Product Integration Laboratories (PIL)</b> .....	26
4.16.1.2	<b>Models, Simulations, Testbeds, and Associated Software</b> .....	26
4.17	Software Engineering.....	27
4.17.1	Software Development Plan (SDP) .....	27
4.17.1.1	<b>Software Safety</b> .....	27
4.17.1.2	<b>Software Quality Inspection Points</b> .....	27
4.17.2	Software Integration and Test Documentation .....	27
4.17.3	Software Transition Planning .....	27
4.17.3.1	<b>C2BMC Planner Transition Plan</b> .....	27
4.17.4	Software Installation Planning.....	28
4.17.5	Software Maintenance Planning .....	28
4.17.6	Control and Management of Software Processes .....	28
4.17.6.1	<b>Software Data / Supporting Information</b> .....	28
4.17.6.2	<b>Software Release Schedules</b> .....	28
4.17.6.3	<b>Software Metrics</b> .....	28
4.17.7	Software Problem Review, Prioritization, and Solution Implementation.....	29
4.17.7.1	<b>Software Change Report (SCR) Tracking System</b> .....	29
4.17.7.2	<b>Program Report Database (PRD) with Software Problem Reports (PRs)</b> 29	29
4.17.8	Post-Deployment Software Support (PDSS) Maintenance Activities .....	29
4.17.9	Software Prototyping .....	30
4.17.10	C2BMC Planner Hosting .....	30
4.17.11	Software Test Environments.....	30
4.17.11.1	<b>Access and Support to Independent Verification and Validation (IV&amp;V) Agent</b> 30	30
4.17.12	Open Architecture.....	30
4.17.12.1	<b>Software Reuse</b> .....	30

<b>4.17.12.2</b>	<b>Commercial Off The Shelf/Non-Development Items (COTS/NDI)</b> .....	30
4.18	Configuration Management (CM) .....	31
4.18.1	Configuration Identification and Documentation .....	31
<b>4.18.1.1</b>	<b>Functional Baseline and Allocate Baseline Documentation</b> .....	31
<b>4.18.1.2</b>	<b>Product Baseline Documentation</b> .....	31
<b>4.18.1.3</b>	<b>Breakout Item(s)/Spare Parts Documentation</b> .....	31
4.18.2	Configuration Change Control.....	32
4.18.3	Configuration Status Accounting.....	32
4.18.4	Configuration Reviews and Audits.....	32
4.18.5	Data Management .....	32
4.18.6	C2BMC Element Configuration Database.....	33
4.18.7	BMDS Core Standards Compliance .....	33
4.19	Information Assurance (IA) .....	33
4.19.1	IA Program Management.....	34
4.19.2	Management Practices .....	34
<b>4.19.2.1</b>	<b>Interfaces</b> .....	34
<b>4.19.2.2</b>	<b>Planning</b> .....	34
<b>4.19.2.3</b>	<b>Reporting</b> .....	34
<b>4.19.2.4</b>	<b>IA Engineering</b> .....	34
<b>4.19.2.5</b>	<b>Architecture Updates</b> .....	35
<b>4.19.2.6</b>	<b>Design Updates</b> .....	35
<b>4.19.2.7</b>	<b>Change Management</b> .....	35
<b>4.19.2.8</b>	<b>Change Proposals</b> .....	35
<b>4.19.2.9</b>	<b>Test Support</b> .....	35
<b>4.19.2.10</b>	<b>Notice and Event Analysis and Response</b> .....	35
4.19.3	DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (DIP).....	36
4.19.4	IA Risk Management .....	36
4.19.5	IA Technology Refresh.....	36
4.19.6	DIACAP Artifact Development.....	37
4.19.7	Plan of Action and Milestones (POA&Ms) Development .....	37
4.19.8	Certification Test and Evaluation (CT&E) Test Development.....	37
<b>4.19.8.1</b>	<b>IA Operations</b> .....	38
<b>4.19.8.2</b>	<b>Site Assistance Visits Support</b> .....	38
<b>4.19.8.3</b>	<b>Controls Validation Testing Support</b> .....	38
<b>4.19.8.4</b>	<b>External IA Assessments and Joint Interface Testing Support</b> .....	38
4.19.9	Information Assurance Officer Support.....	39
4.19.10	Information Assurance Training .....	39
4.19.11	Information Assurance Vulnerability Management (IAVM) .....	39
4.19.12	Computer Network Defense .....	39
4.19.13	Security and Architecture Integration.....	40
4.20	Security Engineering.....	40
4.20.1	Security Management .....	40
4.20.2	Security Requirements Traceability Matrix.....	40
4.20.3	IA Design Activities .....	40
4.20.4	IA Engineering.....	41

4.20.5	IA Architecture Development.....	41
4.20.6	IA Risk Management .....	41
4.20.7	IA Vulnerabilities Mitigation.....	42
4.20.8	IA Configuration Management.....	42
4.20.9	C2BMC Operations Security (OPSEC) Plan.....	42
4.20.10	Anti-Tamper (AT) Techniques .....	42
4.20.11	Certification and Accreditation.....	42
4.20.12	Network Connections.....	43
4.20.13	Reporting.....	43
4.21	Engineering and Technical Services for Production and Deployment Support .....	44
4.22	Facility and Data Access.....	44
4.23	Future Activities Transition .....	44
4.23.1	Advanced Concepts & Technology Evaluation .....	44
4.23.2	Long Lead Architecture, Algorithm, Experimentation, and Engineering Support.....	45
	<b>4.23.2.1 X-Lab Activities .....</b>	<b>45</b>
5.0	SYSTEM TEST AND EVALUATION.....	45
5.1	System Testing.....	45
5.1.1	System Test Planning.....	45
5.1.2	System Test Coordination of Planning, Execution, and Analysis .....	45
5.1.3	Technical Support to Testing .....	46
5.1.4	Test Readiness Reviews (TRR) .....	46
5.1.5	Ground Test Conduct, Range Simulation, and Analysis .....	46
5.1.6	Data for Joint Analysis Team (JAT).....	46
5.2	Sensor Interface Operations .....	46
5.3	Contractor Support to Government Ground Testing .....	46
5.4	Contractor Support to Government Flight Testing .....	47
5.5	BMDs Test Incident Reports (BTIRs) .....	47
6.0	QUALITY, SAFETY, AND MISSION ASSURANCE (QSMA).....	47
6.1	Quality Assurance (QA) .....	47
6.1.1	Quality Assurance Program Plan (QAPP) .....	47
6.1.2	Missile Defense Agency Assurance Provision (MAP) and Parts, Materials, and Processes Mission Assurance Plan (PMAP) .....	47
6.1.3	Mission Assurance Implementation.....	48
	<b>6.1.3.1 Material Review Board (MRB) Authority.....</b>	<b>48</b>
	<b>6.1.3.2 Maintenance and Availability of Quality Records.....</b>	<b>48</b>
	<b>6.1.3.3 Shipping Readiness and Deployment .....</b>	<b>48</b>
	<b>6.1.3.4 System Certification.....</b>	<b>48</b>
	<b>6.1.3.5 Software Qualification.....</b>	<b>49</b>
6.1.4	C2BMC Element Hardware and Software Acceptance .....	49
6.1.5	Software Quality Assurance (SQA).....	49
6.1.6	Quality Metrics .....	49
6.2	Reliability, Availability, & Maintainability Program .....	50
6.2.1	Joint Reliability and Maintainability Evaluation Team (JRMET).....	50
6.2.2	C2BMC Reliability, Availability, and Maintainability Modeling .....	50
6.2.3	Failure Reporting Analysis and Corrective Action System (FRACAS).....	50
6.2.4	Failure Modes Effects and Criticality Analysis (FMECA).....	51

6.2.5	Element Fault Detection, Fault Isolation .....	51
6.3	Parts, Material, and Processes.....	51
6.3.1	Counterfeit Part Avoidance/Mitigation.....	51
6.3.2	Parts Obsolescence.....	51
6.3.2.1	<b>Obsolescence Identification</b> .....	51
6.3.2.2	<b>Obsolescence Mitigation Implementation</b> .....	52
6.3.3	Bill of Materials Management .....	52
6.4	Safety Engineering.....	52
6.4.1	System Safety.....	52
6.4.1.1	<b>Program Safety</b> .....	52
6.4.1.2	<b>Safety Assessments &amp; Analyses</b> .....	53
6.4.1.3	<b>Review of Changes/Problems</b> .....	53
6.4.1.4	<b>Safety Verification</b> .....	53
6.4.2	Safety and Occupational Health.....	53
6.4.2.1	<b>Occupational Health and Safety</b> .....	53
6.5	Environmental Management.....	54
6.5.1	Environmental Laws .....	54
6.5.1.1	<b>Environmental Analysis Reporting</b> .....	54
7.0	<b>SPIRAL OPERATIONS, SUSTAINMENT, AND SYSTEM DEPLOYMENT</b> .....	54
7.1	Operations.....	54
7.1.1	Operations and Maintenance.....	55
7.1.2	C2BMC Asset Management .....	56
7.1.3	C2BMC Sensor Interface Operations & Maintenance.....	56
7.1.4	C2BMC BMDS Network Operation & Security Center.....	56
7.1.5	Site Lead .....	56
7.1.6	C2BMC Control Center (CUBE).....	57
7.1.7	Test Support .....	57
7.2	Sustainment.....	57
7.2.1	Logistics.....	57
7.2.1.1	<b>Maintenance Planning</b> .....	57
7.2.1.2	<b>Supply Support Planning</b> .....	57
7.2.1.3	<b>Item Unique Identification (IUID) Requirements</b> .....	57
7.2.1.4	<b>Support Equipment/Test Measurement and Diagnostic Equipment (SE/TMDE)</b> .....	57
7.2.1.5	<b>Packaging, Handling, Storage, and Transportation (PHST)</b> .....	58
7.2.1.6	<b>Computer Resource Support Planning</b> .....	58
7.2.1.7	<b>Manpower and Personnel</b> .....	58
7.2.1.8	<b>Facilities</b> .....	58
7.2.1.9	<b>Design Interface</b> .....	58
7.2.2	Sustaining Engineering .....	58
7.2.2.1	<b>Technical Refresh</b> .....	58
7.2.2.2	<b>System Enhancements</b> .....	58
7.2.3	Training, Training Media and Training Devices .....	58
7.2.4	Technical Data .....	59
7.3	System Deployment.....	59
7.3.1	System Deployment and Site Activation .....	59

7.3.1.1	<b>Fielding Engineering</b> .....	59
7.3.1.2	<b>System Activation Process</b> .....	59
7.3.1.3	<b>Fielding Activities</b> .....	59
7.3.1.4	<b>Fielded Hardware Lists</b> .....	60
7.3.1.5	<b>Decommissioning &amp; Disposal</b> .....	60
8.0	WARFIGHTER INTEGRATION .....	60
8.1	Wargames and Exercise Support .....	60
8.2	Friends and Allies Support.....	60
8.3	Warfighter User System Modification Request.....	60
8.4	Human Factors Engineering (HFE) Working Group.....	60
9.0	BMDS COMMUNICATION & NETWORK DEVELOPMENT.....	61
9.1	Government Furnished Long-Haul Communication Services.....	61
9.1.1	Interface Control Specification .....	61
9.2	Network Development .....	61
9.3	Network Concepts & Requirements .....	62
9.4	Information Exchange Requirements (IER) .....	62
9.5	Network Model .....	62
9.6	Network Design .....	63
9.6.1	Network Security Design.....	63
9.6.2	Network Trades.....	63
9.7	Network Integration & Test.....	63
9.8	Network System Integration and Test Environment (NSITE).....	64
9.9	Trouble Ticketing/ Work flow System .....	64
9.10	Data Collection and Analysis.....	64
10.0	CONCURRENT TEST, TRAINING AND OPERATION (CTTO) .....	64
11.0	SUPPORT REAL WORLD OR CONTINGENCY OPERATIONS .....	64
12.0	Places of Performance.....	65
13.0	Acronym List .....	69

## **1.0 SCOPE**

### **1.1 General**

The core Command and Control, Battle Management and Communications (C2BMC) Program is an Element of the Ballistic Missile Defense System (BMDS). The C2BMC program is responsible for the end-to-end mission communications network connectivity between BMDS elements, Combatant Commanders (COCOMs), Services and agencies. The C2BMC System, through the BMDS Communications Network (BCN), links together the external sensors and weapons of independent Elements into a layered missile defense system such that the whole is far more capable and robust than the sum of its parts -- thus increasing the capability of the BMDS with greater performance and defensive coverage. The C2BMC System enables the BMDS to manage complex threats -- near simultaneous enemy missile shots aimed at theater, regional, or homeland assets. The C2BMC System includes the communications network capability that is required to support the C2BMC functionality, Information Assurance (IA) enhancements (architecture, monitoring, correlation), and the movement of data and information within the C2BMC System's applications (i.e., the network capability specifically tied to the execution of the core C2BMC capability).

The scope of work identified in this contract requires a collaborative enterprise comprised of the best and most experienced personnel from Industry and Government. The team shall operate as an integrated high performance team, maintaining a product-oriented focus and working from a common Statement of Work. In this environment, all activities shall be collaborative with open interaction across the entire Government and Industry Team. To the maximum extent allowed by the Federal Acquisition Regulations (FAR), Department of Defense FAR Supplement (DFARS), and other Department of Defense (DOD) regulations and MDA policies and procedures, the Prime Contractor shall continue to work utilizing an "Alpha Engineering" process that leverages the experience of the entire team to acquire the best product regardless of affiliation.

### **1.2 Specific Terms and Definitions**

The term "Contractor" refers to the overall prime/sub-team under the management and control of the prime Contractor. In this regard, the prime Contractor is responsible for flowing down Statement of Work (SOW) requirements to Subcontractors and to arrange for Subcontractor participation as necessary and appropriate to assure the efficient, effective and successful performance of all SOW requirements.

### **1.3 C2BMC Element**

The Contractor shall develop, model, fabricate, integrate, test, verify, evaluate, validate, document, deliver, field, train, operate, sustain, and support updates and new capabilities to the C2BMC Element. The Contractor shall develop C2BMC operational, sustainment and training capabilities within each spiral hardware and software drop to the field and System Engineering support to C2BMC test events and exercises, as defined in task orders.

## **2.0 APPLICABLE DOCUMENTS**



## **2.1 Compliance Documents**

- a) **Deleted**
- b) DoDD 8500.01 Cybersecurity, 14 March 2014.
- c) **Deleted**
- d) DoDI 8510.01 DoD Risk Management Framework (RMF) for DoD Information Technology
- e) DoDI 5220.22-M National Industrial Security Program Operating Manual (NISPOM), February 28, 2006 incorporating change March 28, 2013.
- f) **Deleted**
- g) BALLISTIC MISSILE DEFENSE SYSTEM GROUND TEST CONCEPT OF OPERATIONS MDA INSTRUCTION 3000.07-INS December 3, 2012 Administrative Change 1, March 4, 2013; BALLISTIC MISSILE DEFENSE SYSTEM FLIGHT TEST CONCEPT OF OPERATIONS MDA DIRECTIVE 3000.10 June 13, 2014
- h) MDA DIRECTIVE 3002.03 Ballistic Missile Defense System Test Policy, 21 June 2010.
- i) MDA DIRECTIVE 5000.04 Program Change Board, 02 October 2009.
- j) MDA DIRECTIVE 5010.18 Acquisition Management, 29 April 2011.
- k) MDA DIRECTIVE 9315.01 Modeling And Simulation (M&S), Verification, Validation, and Accreditation (VV&A), 21 January 2009, Incorporating Change 1, 6 April 2011.
- l) MDA DIRECTIVE 5000.05 – Single Technical Authority, September 25, 2013
- m) MDA INSTRUCTION 3058.01-INS – Risk Management, 15 April 2011.
- n) **Deleted**
- o) BMDS Adversary Data Package for BMDS Integrated Build D Addendum 1, European Capability Revision A, 12 June 2008.
- p) MDA Instruction 8430.01-INS Software Acquisition, 30 Oct 2013
- q) DODI 8510.01 RMF for DoD Information Technology, 12 March 2014
- r) DoDI 8551.01 Ports, Protocols, and Services Management (PPSM), 28 May 2014
- s) CNSSI 1253 Security Categorization and Control for National Security Systems, 27 March 2014
- t) DoD CIO Memorandum - Mandates Implementation of NIST 800-147, BIOS Protection Guidelines, on DoD Information Systems, 1 April 2011
- u) CNSSI 1253A Implementation and Assessment Procedures, 27 March 2014
- v) DoD 5200.2 Personnel Security Program, Change 3, 24 February 1996

## **2.2 Guidance Documents**

### **2.2.1 Department of Defense Documents**

- a) Secretary of Defense Memorandum for Missile Defense Program Direction, 2 January 2002.
- b) DoDD O-8530.1 Computer Network Defense (CND), 08 January 2001.
- c) DoDI 6055.1 Department of Defense Safety and Occupational Health Program, 19 August 1998.
- d) DoD 8570.01-M Information Assurance Workforce Improvement Plan, Incorporating Change 3, January 24, 2012.
- e) CJCSI 6510-01F Information Assurance (IA) and Computer Network Defense (CND), 09 February 2011.
- f) DoDI 8580.1 Information Assurance (IA) in the Defense Acquisition System, 09 July 2004.

- g) CJCSM 6510.01 Cyber Handling Program, 10 July 2012.
- h) CJCSI 3210.01C Joint Information Operations Policy 14 February 2014.
- i) DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing, April 12, 2006.
- j) GIG TG Federation (<https://gtg.csd.disa.mil>) Software Release 1.11.34, 28 October 2015. Deleted
- k) MIL-STD-188-125-1 High-Altitude Electromagnetic Pulse (Hemp) Protection For Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions Part 1 Fixed Facilities, 17 July 1998, validated current 07 April 2005.
- l) MIL-STD-188-125-2 High-Altitude Electromagnetic Pulse (Hemp) Protection For Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions Part 2 Transportable Systems, 3 March 1999, validated current 07 April 2005.
- m) MIL-STD-461F Requirements for the Control of Electromagnetic Interface Characteristics of Subsystems and Equipment, 10 December 2007.
- n) MIL-STD-464C Department of Defense Interface Standard: Electromagnetic Environmental Effects Requirements for Systems, 01 December 2010.
- o) MIL-STD-810G Department of Defense Test Method Standard, ENVIRONMENTAL ENGINEERING CONSIDERATIONS AND LABORATORY TESTS, 15 April 2014.
- p) MIL-STD-882C Standard Practice for System Safety Revision C, 19 January 1993, Change Notice 1, 19 January 1996.
- q) MIL-STD-1366E Transportability Criteria, 31 October 2006.
- r) MIL-STD-1472F(1) Department of Defense Design Criteria Standard: Human Engineering, 23 August 1999, Change Notice 1 05 December 2003.
- s) MIL-STD-2525C Common Warfighting Symbolology, 17 November 2008.
- t) MDA-STD-007, BMDS Data Link Standards Baseline Change 1, 17 July 2014
- u) MIL-STD-6040B(1) NOT 1, United States Message Text Formatting Program (USMTF), 30 April 2009, Revision B Change 1, 31 January 2011.
- v) MIL-HDBK-310 Global Climate Data for Developing Military Products, 23 June 1997.
- w) TB 700-2 DoD Ammunition and Explosives Hazard Classification Procedure, 30 July 2012.
- x) TM 38-250 DoD – Preparing Hazardous Materials for Military Air Shipments, 15 April 2007, Incorporating Change 1, 4 May 2007.
- y) **Deleted**
- z) MIL-HDBK-1791(2) Designing for Internal Aerial Delivery in Fixed Wing Aircraft, 2 December 2014.
- aa) Technical Manual 5-691 (Utilities for C4ISR Facilities), 27 December 2006.
- bb) Technical Manual 5-693 (UPS for C4ISR Facilities), 26 December 2007.
- cc) Network Infrastructure, Security Technical Implementation Guide (STIG), Version 8, Release 7, 25 August 2014.
- dd) MIL-HDBK-245D, DoD Handbook for Preparation of Statement of Work, 3 April 1996.
- ee) DoD Architecture Framework Version 2.02, August 2010.
- ff) DoDM 5200.01, Volume 1 DoD Information Security Program: Overview, Classification, and Declassification

- DoDM 5200.01, Volume 2 DoD Information Security Program: Marking of Classified Information
- DoDM 5200.01, Volume 3 DoD Information Security Program: Protection of Classified Information
- DoDM 5200.01, Volume 4 DoD Information Security Program: Controlled Unclassified Information (CUI)
- gg) Under Secretary of Defense (USD) (AT&L) MEMORANDUM FOR ACQUISITION PROFESSIONALS: Better Buying Power: Guidance for Obtaining Greater Efficiency and Productivity in Defense Spending, 14 September 2010.
- hh) Secretary of Defense Memorandum for Missile Defense Program Direction, 2 January 2002.
- ii) CJCSI 6211.02c, Defense Information Systems Network (DISN) Policy and Responsibilities, 24 January 2012.
- jj) MIL-HDBK-1785, "System Security Engineering Program Management Requirements," 1 August 1995, Valid as of 22 April 2014.
- kk) DISA Circular 310-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards, 30 October 2009.
- ll) DoD Memorandum Open Source Software in the Department of Defense, 2009

### **2.2.2 Missile Defense Agency (MDA) Documents**

- a) S-0637-1.0 Integrated BMDS Build D Internal BMDS Interface Control Document: Part 1(U), 20 May 2014 + DCN's 40, 41, 42
- b) Integrated BMDS Build D SBIRS BMD System Interface Control Document: Part 1 (Classified Document), 23 December 2009
- c) BMD System Description Document v15.3 (Classified Document), 19 May 2015
- d) BMDS Build D Internal Interface Control Document: Part 2, Volume 1: General and Link 16 Formatted Data (Classified Document), 25 June 2012
- e) BMDS Build D Internal Interface Control Document: Part 2, Volume 1, Classified Supplement: Appendices A-E (Classified Document), 25 June 2012
- f) BMDS Build D Internal Interface Control Document: Part 2, Volume 2: GMD and C2BMC (Classified Document), 14 May 2014
- g) Missile Defense Agency (MDA) Integrated Master Test Plan (IMTP) (Classified Document)
- h) BMDS Master Plan Version 9.1, 15 April 2009.
- i) **Deleted**
- j) MDA Directive 5200.01 Security Policy, 10 June 2012
- k) MDA Directive 5200.05 Anti-Tamper Policy, 1 June 2012
- l) MDA-QS-001-MAP, MDA Assurance Provisions Revision A, 29 October 2006.
- m) MDA-QS-003-PMAP, MDA Parts, Materials and Processes Mission Assurance Plan Revision A, 26 March 2008.
- n) MDA DIRECTIVE 8315.02 Modeling and Simulation Program, 13 January 2009, Change 1, 6 April 2011.
- o) BMDS Security Classification Guide, 26 April 2004, updated 19 October 2010 to include Admin Changes 11 July 2011
- p) MDA Information Assurance Plan 8500.02-P, 3 October 2007.

- q) BMDS Adversary Data Package (ADP) for Integrated BMDS Build D, Rev A, (Classified Document), 12 June 2008
- r) BMDS Analysis Reference Architecture, 31 March 2011.
- s) C2BMC Build D Element Specification (Classified Document, 15 April 2014
- t) C2BMC-AOC Mutual Commitment Package, November 2008.
- u) Warfighter BMDS Modification Request List, 29 August 2006.
- v) **Deleted**
- w) **Deleted**
- x) SS0017 Space Based Infrared System (SBIRS) Ground to Ballistic Missile Defense System (BMDS)
- y) Cost Analysis Requirements Description (CARD) MDA Handbook Version 12, 14 November 2013
- z) BMDS System Engineering Plan Revision 1.0, 29 April 2011
- aa) MDA Directive 4122.01 Ballistic Missile Defense Systems Core Standards, 21 June 2011.
- bb) MDA Directive 6055.04-INS Work Time Restrictions for Safety and Mission Critical Personnel Supporting Tests and Critical Operations, 27 August 2012
- cc) MDA Directive 4245.01 Metrics Program, October 2008.
- dd) MDA Manual 3500.01-M BMDS Change Management Process, 23 Oct 2013, Change 1, 14 Jan 2014
- ee) DRAFT BMDS Schedule PAA Phase 2, 26 Feb 2014
- ff) **Deleted**
- gg) MDA JRMET Charter, 23 July 2014.
- hh) MDA Instruction 6055.02-INS Accident and Mishap Safety Investigations and Reporting, 22 May 2013
- ii) **Deleted**
- jj) **Deleted**
- kk) BMDS Integrated Master Assessment Plan (IMAP), Version 13.1 (Classified Document), 31 May 2013

### **2.2.3 Other Government Documents**

- a) 47 Code of Federal Regulations – Part 15: Radio Frequency Devices, 20 October 2014
- b) ICAO Doc 9284 Internal Civil Aviation Organization Technical Instructions for the Safe Transport of Dangerous Goods by Air, Corrigendum No.3, 13 December 2013
- c) International Maritime Dangerous Goods (IMDG) Code Amendment 37, 10 June 2014
- d) NSTISSAM 2-95 NOAA Data National Oceanic and Atmospheric Administration Global Summary of the Day, Current Model "NSTISSAM Tempest, 17 Jan 2014
- e) National Security Systems Policy 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products," June 2013
- f) OMB Circular No.A-130, 30 November 2000.
- g) Public Law 100-235, Computer Security Act of 1987, 8 January 1988.
- h) Federal Information Security Management Act (FISMA), 2002.
- i) Army in Europe Regulation AE 715-9, 10 September 2009
- j) NSTISSAM TEMPEST/1-92, 15 December 1992.
- k) NSTISSI 7001 NONStop Countermeasures, 15 June 1994

l) **Deleted**

- m) IEEE 12207 Software Life Cycle Processes, 15 April 2011.
- n) AMCOM Regulation (AR) 385-17, 15 March 2008.
- o) NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4, April 2013
- p) NIST 800-27A Engineering Principles for Information Technology Security (A baseline for Achieving Security, June 2004  
DoD Memorandum Open800-70
- q) NIST 800-30 Rev 1 Guide for Conducting Risk Assessments, September 2012
- r) NIST 800-100 Information Security Handbook: A Guide for Managers, October 2006
- s) Modular Open Systems Approach (MOSA), 29 September 2004.
- t) ANSI/EIA-748-C Standard for Earned Value Management Systems Intent Guide, 29 April 2014
- u) NIST SP 800-37 Guide for Applying the RMF to Federal Systems: A Security Life Cycle Approach, February 2015
- v) NIST SP 800-53A Guide for Assessing the Security Controls in Federal Information Systems: A security Life Cycle Approach, December 2015
- w) NIST SP 800-61 Rev 2 Computer Security Incident Handling Guide, August 2015
- x) NIST SP 800-64 Rev 2 Security Considerations in the System Development Life Cycle, October 2015
- y) NIST SP 800-137 Information Security Continuous Monitoring, September 2015
- z) NIST SP 800-160 System Security Engineering, May 2015
- aa) NIST 800-147 BIOS Protection Guidelines, April 2015
- bb) NIST SP 800-70 Rev 2 National Checklist Program for IT Products-Guidelines for Checklist Users and Developers, February 2015
- cc) CNSSAM TEMPEST 1-13 Red Black Installation Guide, 17 January 2014

**2.3 Contractor Documents & Industry Standards, Specifications, and References**

Contractor Documents provided in Contractor Statement of Work (CSOW)

All current BMDSS Builds documentation, to include Builds from previous efforts.

**3.0 PROGRAM MANAGEMENT**

The Contractor shall provide program management services to enable planning, controlling, directing, monitoring, reporting, and managing in a manner consistent with SOW requirements.

All documentation created and maintained in a database or storage medium associated with this contract shall be delivered to the Government by the various CDRLs associated with this contract. This information shall be delivered to the Government in a format equal to what was previously used in Agreement No. HQ0006-02-9-0002, to include what was used by the contractor, unless otherwise noted within the individual CDRLs.

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.

### **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 cost, schedule, performance, and supportability requirements for C2BMC hardware/software.

### **3.2 Contractor Integrated Performance Management**

The Contractor shall prepare and utilize, in the performance of this contract, an integrated performance management system. Central to this integrated system shall be a DoD validated Earned Value Management System (EVMS), compliant with the EVMS guidelines contained in ANSI/EIA-748-B. To establish the integrated performance management system, 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. The correlation and integration of these systems and processes shall provide for early indication of cost and schedule problems, and their relation to technical achievement.

### **3.3 Integrated Baseline Reviews (IBRs)**

The Contractor shall engage jointly with the Government's program manager and his representatives in IBRs to evaluate the risks inherent in the contract's planned performance measurement baseline. The totality of the baseline may 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), is consistent with contract schedule requirements, and has adequate resources assigned. Each IBR shall record any indications that compliant Earned Value Management (EVM) is not being used. Each IBR shall contain integrated subcontract data.

### **3.4 Integrated Master Schedule (IMS)**

The Contractor shall prepare a C2BMC IMS by logically networking detailed program activities. The schedule shall contain the C2BMC Integrated Master Plan (IMP) consistent with the BMDS IMS that lists the activities and resources required to achieve the C2BMC Spiral capabilities. The IMS shall be prepared In Accordance With (IAW) DI-MGMT-81650 (CDRL-A002). The Contractor shall provide primary, secondary, and tertiary critical path analysis at the IMS network level. The Contractor shall have written Government approval prior to incorporating any tier 1, 2, 3, or 4 schedule baseline changes to the IMS.

### **3.5 Process Control**

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

### **3.6 Program Reviews**

The Contractor shall plan, prepare for, conduct, and provide minutes of program reviews IAW DI-MGMT-80368A (CDRL-A003).

### **3.7 Subcontract Management**

The Prime Contractor (Lockheed Martin) shall manage and coordinate the tasks among the subcontractors and team members by using a subcontract management plan. The Contractor shall prepare and deliver a Small Business Participation/Utilization Report IAW DI-MGMT-81642 (CDRL-A024).

### **3.8 Contract Work Breakdown Structure (CWBS)**

The Contractor shall prepare and deliver the CWBS and CWBS dictionary IAW DI-MGMT-81334D (CDRL-A004) and any additions to them, throughout the life of this contract. The Contractor shall provide a mapping of their Contract WBS to the Agency's Common Work Breakdown Structure (WBS), the Program WBS, by WBS element code.

### **3.9 Contract Performance Report (CPR)**

The Contractor shall prepare, maintain, and deliver a CPR IAW DI-MGMT-81466A (CDRL-A005).

### **3.10 Contract Funds Status Report (CFSR)**

The Contractor shall prepare, maintain, and deliver a CFSR IAW DI-MGMT-81468 (CDRL-A006).

### **3.11 Cost Working Group (CWG)**

The Contractor shall support the C2BMC CWG. The Contractor shall support the Common Cost Model development as described in Missile Defense Agency (MDA) Directive 4250.02 BMDS Cost Estimates. The Contractor shall deliver Common Cost Model inputs IAW MDA Directive 4250.02.

### **3.12 Cost Analysis Requirements Description**

The Contractor shall support the development of the Cost Analysis Requirements Description, (CARD) by providing inputs to the Government IAW MDA Card Handbook.

### **3.13 Cost and Software Data Reporting (CSDR)**

#### **3.13.1 Cost Data Reporting**

The Contractor shall prepare, maintain, and deliver the Cost Data Summary Report (DD Form 1921) IAW DI-FNCL-81565C (CDRL-A009) and the Functional Cost-Hour and Progress Curve Report (DD Form 1921-1) IAW DI-FNCL-81566C (CDRL-A010).

#### **3.13.2 Software Data Reporting**

The Contractor shall prepare and deliver the Software Resources Data Reporting IAW DI-MGMT-81739B (CDRL-A045). The Software Resources Data Reporting includes the Initial Developer Report, the Final Developer Report, and the Data Dictionary.

### **3.14 Risk and Opportunity Management**

The Contractor shall manage, execute and maintain a risk and opportunity management program for the C2BMC Element in accordance with MDA Risk Management Instruction

3058.01-INS (April 15, 2011) and as implemented in the Contractor's Risk and Opportunity Management Plan.

- a. The Contractor shall review the plan annually with MDA and update as necessary.
- b. The Contractor shall allow for the identification, management, and adjudication of risks, issues, and opportunities by all members identified in the Risk and Opportunity Management Plan.
- c. The Contractor shall manage and track internal (C2BMC) and external (MDA/other Element) risks and opportunities.
- d. The Contractor shall report the status of C2BMC Element risks to the Government on a regular basis and request feedback and guidance as necessary. The Government will provide feedback and guidance as requested in time for consequential actions to be performed in a timely fashion.
- e. The Contractor shall participate in and support the Government led Risk Management Working Groups (RMWGs), the Chief Engineer's Risk Management Board, and other reviews as necessary to accomplish the risk management mission.

### **3.15 Searchable Repository**

The Contractor shall implement, and continuously secure, a C2BMC searchable repository IAW DI-IPSC-81437 (CDRL-A025). All efforts shall be made to utilize Government resources to include Government owned networks, specifically MDA Unclassified Network (MDAUnet) if available, and if it is the most cost effective solution, for use of unclassified information development. All of the documentation maintained in any online searchable repository and linked information in support of this contract, shall be delivered to the Government at the conclusion of this contract or upon request by the Government contracting officer, for historical purposes.

The Contractor shall ensure that the C2BMC searchable repository contains all technical data to support the Joint Government/Contractor engineering management of the C2BMC architecture design, network and software development environment (SDE) including all systems life cycle processes. The Contractor shall include all technical data associated with architecture design, requirements development, software development, and C2BMC deliverables within the C2BMC searchable repository including the following:

- a. C2BMC Architecture Artifacts: The Contractor shall provide weekly updates of the C2BMC Spiral Architecture Artifacts (Use Cases, Activity and Sequence Diagrams) that define the C2BMC Sub-System/Component structure and behavior requirements.
- b. Dynamic Object Oriented Requirements System (DOORS) Requirements Database: The Contractor shall provide weekly updates from the DOORS Requirements Database for the Government Configuration Control Board approved Spiral Technical Baseline. (Ref: The contractor shall be responsible for ensuring that all products including software, whether acquired from a third party or produced by the contractor and delivered under this task order, is suitable for its intended purpose and performs as specified in the performance specifications. Prior to delivery, the contractor shall provide documented evidence to the government that adequate testing to confirm



suitability and performance has been performed by the contractor, or by a third party on the contractor's behalf, before the government will provide formal acceptance of that product. Formal requests for exceptions to this requirement must be submitted in writing by the contractor to the government, and will be evaluated on a case by case basis by the government with no obligation on the government's part to grant an exception. The contractor shall maintain all related documentation for the life of the contract, and are deliverable items to the government upon request. Para 4.5)

- c. Software Development Folders (SDFs): The Contractor shall create and maintain an automated, searchable repository of both current and historical C2BMC software development information, whether in the same database used for the integrated data or another database linked to the searchable repository. Several forms of data are created during software development:
- Current and historical software engineering data developed within the appropriate tool (e.g., within DOORS, ClearCase).
  - Notes, presentations and snapshots of selected data, such as requirements reports, design rationale, or design representations, to facilitate review of in-progress natural products by users unfamiliar with the tools or at locations separate from the tools.
  - SIL Management Plan IAW DI-SESS-81770
  - Outputs of evaluations and formal reviews.
  - Formal documents to establish the developmental configuration, test configuration, and Functional Area (FA) product baselines.

The types of data identified in the following table are candidates for the Software Development Folder (SDF):

System/Subsystem Identification	Any general document describing the system or subsystem with link to the subsystem decomposition as appropriate.
Points of Contacts	List of architects with their associated domains.
Development Schedules	Reference to Development (DEV) schedule location.
Spiral Content	Description of the set of functionality for the spiral.
Software or Task Requirements	Requirements shall be maintained in DOORS. The SDF shall contain a pointer to the DOORS database. List of all related Configuration Management (CM) packages. Source code files are listed and maintained in IBM Rational DOORS for ClearCase Interface 2.1.1. Rational Rhapsody 7.5
Software Requirements Decisions & Rationale	Any important document supporting the rationale for the subsystem derived requirements.
Use Case Extension	Any extension of the subsystems use case developed by Architecture & System Engineering (A&SE) (reference if the use cases are kept in a central location).
Results of Software Reviews of Derived Requirements	Work Product Inspections (WPIs) for the derived requirements.

Software Design (e.g., architecture, behavior, detailed)	Charts used for design Technical Interchange Meeting (TIM), including design rationale, and Functional Area Design Description (FADD).
FADD per Appropriate Design Document Template	Includes: <ul style="list-style-type: none"> <li>- Context Diagram showing the interface between the subsystems and other subsystems or external elements.</li> <li>- Interfaces between the subsystem and other subsystems or external elements. Since all inter-subsystems interface are defined at the top-level SDF, only references are required here. For external interfaces, a reference to the appropriate Interface Design Documents (IDDs) should be provided.</li> <li>- Description of the subsystem decomposition into component and a component description.</li> <li>- Reference to all critical methods used by this subsystem.</li> </ul>
Top-Level Diagrams	Diagram describing the logical and physical architecture as well as site-specific diagrams.
Peer Review Results	Peer Review for the top-level diagrams.
Cross-Subsystem Interfaces	Interfaces for libraries or services used across subsystems such as control & monitoring, time reference or logging.
External Message Format	Reference to external IDDs or Interface Control Documents (ICDs).
Internal Message Format	Reference to the CM location of the internal message description.
Peer Review Results	WPIs for the internal message format.
Architecture Notes	Any other document relevant to the architecture.
Trade Studies	Report on Architecture trade studies.
Results of Software Evaluations of the Source Code	Peer reviews for the subsystem code.
Checklists	Checklists for Peer Reviews and Exit Readiness Assessments.
Software Test Decisions and Rationale	Documents describing special unit test needs for the subsystems (ex: automated message tester in Message Processing (MP) or Benchmark validation for Track Server).

Software Unit Test Material	Points to the automated build report tool. For Quality Assurance (QA) purposes may contain snapshot of unit test results at critical development point.
Integration Plans, Presentations, or Information	Document describing special integration needs for the subsystem.
Software Integration Test Material – Plans, cases, procedures, data, analysis results	Contains or points to location of integration test materials.
Software Developer Notebook	Any document not listed above that is relevant to the comprehension or the maintenance of this subsystem.

- d. Software Modification Requests (SMRs): The Contractor shall create and maintain an automated, searchable repository of both current and historical C2BMC System Modification Requests (SMRs). As described in SMR procedure PR-PM-0048, a System Modification Request is a broad term used for any request to initiate and track a required or suggested modification to the C2BMC system, including software, hardware, and associated technical documentation. An SMR is opened when a system defect or discrepancy is discovered, or an enhancement is identified.

### **3.15.1 Program Data**

The Contractor shall populate the searchable repository with program data, integrate/migrate any associated program databases, verify data integrity, and develop and use quality control procedures for updates of data available. The Contractor shall support Integrated Product Team (IPT) information needs and integrate team-linking tools for collaboration purposes. At the conclusion of this contract or upon request of the Government Contracting Officer, all data contained in the program databases shall be delivered to the Government, for historical purposes. Further direction on the distribution method will be determined by the Government.

### **3.15.2 Data Access**

Access to C2BMC program data on Contractor-managed systems shall be restricted to both external users and those internal to the Contractor's facility with an established need-to-know. The Contractor shall establish User accounts for external access to the searchable repository access for all Government personnel identified by the C2BMC Program Manager.

#### **3.15.2.1 Unclassified Repository**

The Contractor shall make documents available through a searchable unclassified repository that are compatible with the current standard business suite of software deployed by the Missile Defense Agency to the C2BMC Program Office (MDA/BC), such as the operating system, MS Office suite, and Adobe Reader. The Contractor shall establish connectivity and provide access to the searchable unclassified repository for the major C2BMC facilities, ranges, other Government agencies, and support Contractors, as required.

### **3.15.2.2 Classified Repository**

The Contractor shall provide the same capability, functionality, and oversight as described for the unclassified searchable data repository. The Contractor shall utilize the Missile Defense Agency Classified Network (MDACNet) with high bandwidth connectivity to MDA organizations for productivity enhancements, file sharing, and collaborative user environment in support of the MDA mission of Research, Development, Test, and Evaluation (RDTE). A Contractor-controlled firewall shall be installed when connecting Defense Security Services (DSS) accredited classified systems to the MDACNet IAW PCI Data Security Standard (v 1.2.1). The Contractor shall be required to obtain accreditation and approval for classified connections to MDACNet.

### **3.16 Data Accession List**

The Contractor shall prepare a Data Accession List (DAL) IAW DI-MGMT-81453A/T (CDRL-A012). The Data Accession List shall identify all internal data generated by the Contractor in performance of the contract.

### **3.17 Information Initiatives**

The Contractor shall provide technical and programmatic support to special presentations/information initiatives, which are beyond the regularly scheduled presentations/reviews to the Government. The Contractor shall obtain prior approval from the contracting officer, for each separate presentation/initiative under this paragraph, IAW MDA Public Release Policy. The presentations/initiatives under this paragraph may include, but are not limited to, white papers, newsletters, videotapes, exhibits, Congressional hearings, International Conferences and other related media.

### **3.18 Rough Order of Magnitude (ROM)**

The Contractor shall support program-planning activities by providing ROM estimates, for emerging Government needs. Estimates shall provide sufficient information to determine the reasonableness of the ROM.

## **4.0 SYSTEMS ENGINEERING**

The Contractor shall apply standard Systems Engineering processes to develop, model, fabricate, integrate, test, verify, evaluate, validate, document, deliver, field, train, operate, sustain, decommission and support updates to the existing C2BMC Element. The Contractor shall develop, verify and maintain hardware and software interfaces with other Ballistic Missile Defense (BMD) elements and designated other parties (other US/DOD, NATO, Friends and Allies) and deliver new capabilities in the Spiral 8.2 build.

The Contractor shall provide technical assistance and information to support a Government-chaired Product Integration Team (PIT). The Contractor shall include Government Product Engineers and Subject Matter Experts (SMEs) within the engineering development teams to participate in the Contractor's system and software designs including the following:

- Architecture Design
- Requirements analysis/refinement

- Systems/software engineering and design
- Other activities specifically identified in this SOW

The Contractor shall maintain overall command and decision responsibility over the engineering development teams. Unresolved issues that arise out of the engineering development teams between Government and Contractor personnel shall be presented by the Contractor to the C2BMC Product IPT leadership for dispute arbitration.

#### **4.1 C2BMC Architecture**

The Contractor shall develop and maintain C2BMC Architecture Artifacts (Use Cases, Activity and Sequence Diagrams) that define the C2BMC Sub-Systems/Component structure and behavior requirements. The C2BMC Architecture shall define the derived requirements that will provide the capabilities allocated to C2BMC within the BMD System Specification. The resulting Architecture Artifacts shall be described in a System Architecture and Requirements Allocation Description (SARAD). The Contractor shall make Architecture artifacts available for Government review at all peer reviews, technical interchanges, design reviews and other meetings as requested in the BMDSS Build D Specs IAW DI-MGMT-81644A (CDRL-A026).

The Contractor shall develop and maintain interfaces with other Ballistic Missile Defense (BMD) elements and maintain Interface Control Documents (ICDs) as part of the system engineering process IAW DI-CMAN-81248A (CDRL-A013), and store electronically in the searchable repository.

#### **4.2 C2BMC Build Specifications (CBS)**

The Contractor shall maintain a C2BMC Build Specification and Interface Control Documents (ICDs) traceable to the Ballistic Missile Defense System Specification (BMDSS) Build D, applicable core standards, and System Interface Control Documents (SICDs) IAW DI-MCCR-80700 (CDRL-A014). Traceability shall be maintained to the Build D BMDSS and SICDs for changes to either C2BMC or BMDS documentation. ICD's shall include safety critical interfaces and functions as identified to the Contractor or as identified by C2BMC. The Program Safety section of this SOW contains the definition of safety critical interfaces.

#### **4.3 C2BMC Spiral Specifications (CSS)**

The Contractor shall maintain a C2BMC Spiral Specification traceable to the C2BMC Build Specification and consistent with the BMDSS and applicable SICDs IAW DI-MCCR-80700 (CDRL-A015). Traceability shall be maintained to the C2BMC Build Specifications (CBS), Build D BMDSS, and SICDs for changes to either C2BMC or BMDS documentation.

##### **4.3.1 Integrated Engineering**

The Contractor shall translate CSS requirements into configuration controlled hardware and software Element through a systematic approach to integrated design. The Contractor shall integrate all technical requirements and disciplines into a coordinated effort to meet cost, schedule, performance, affordability, quality, reliability, producibility,

and supportability requirements IAW PL-AS-0001 the C2BMC Architecture and Systems Engineering Management Plan.

#### **4.3.2 System/Software Engineering**

The Contractor shall develop C2BMC Spiral 8.2 (S8.2) to provide for incremental deliveries of ever-increasing capability ultimately fulfilling all CSS requirements. All software executables, source code, tool sets, libraries, licensing provisions and documentation for each increment shall be delivered to the Government in accordance with the C2BMC contract technical data and computer software rights clauses Executables and Source Code IAW DI-IPSC-81441A (CDRL-A042).

The Contractor shall rehost all applicable C2BMC Spiral 6.4C2 (S6.4C2) software functionality IAW C2BMC Element Specification to the re-capitalized S8.2 computing infrastructure.

The Contractor shall ensure C2BMC Network Architecture, Designs and software are in compliance with the requirements of the approved CSS and ICDs. The software detailed design requirements and implementation shall be documented in a Functional Area Design Description (FADD) document and submit to the Government for review IAW DI-MCCR-80700 and DI-SESS-81785 (CDRL-A017).

The Contractor shall conduct a C2BMC S8.2 Critical Design Review (CDR) for the purpose of baselining the C2BMC S8.2 design implementation prior to receiving Government authorization to proceed with final development efforts.

The Contractor shall conduct a peer review for design and code for each new, modified, or existing module. Government Product Engineers and Subject Matter Engineers shall be included as part of each peer review and permitted access to Contractor software development folders.

The Contractor shall develop a C2BMC Operational Concept (OPSCON) Description Document IAW DI-ISPC-81430A (CDRL-A016).

#### **4.3.3 Part 1 and Part 2 Interface Control Document (ICD) Support**

The Contractor shall participate in and support the development of the Interface Control Document (ICD) Part 1 documents developed by the Government. In addition, the Contractor shall establish and maintain ICD Part 2s ensuring traceability to ICD Part 1s. The Contractor shall verify C2BMC performance with applicable Part 2 ICDs, support overall BMDS ICD verification, and support BMDS interoperability issue resolution.

#### **4.3.4 User Interface Engineering**

The Contractor shall execute a human factors engineering (HFE) program during development and acquisition of the C2BMC system to ensure effective integration of personnel in the design of the system. The HFE program will follow guidance provided by MDA, and will also develop, document and follow a process (PR-PM-0001, Human

Factors Engineering Process) to provide structured methods for achieving usability in user interface engineering and design during product development.

#### **4.3.5 High-Altitude Electromagnetic Pulse (HEMP), Electrostatic Discharge (EDS), ENVIRONMENTAL**

The Contractor shall consider BMDSS Core Standards, IAW MDA Directive 4122.01, Dec 2010, and any subsequent updates are addressed during design, development and acquisition of the C2BMC system, as described in the applicable Task Orders awarded for this contract.

#### **4.4 Department of Defense (DoD) Information Technology Standards Registry (DISR)**

The Contractor shall provide technical assistance and information to support the C2BMC technical architecture profile IAW DISR. The Contractor shall provide information that details how the C2BMC Element improvements comply with DISR Information Management requirements.

#### **4.5 Dynamic Object-Oriented Requirements System (DOORS)**

The Contractor shall maintain all data associated with BMDSS Build D, C2BMC Element Specification(s), and C2BMC S8.2 Specification(s), and part 2 ICDs in the DOORS database. C2BMC requirements traceability to the C2BMC S8.2 Specification with subsequent traceability to the BMDSS specification shall be maintained in DOORS. The Contractor shall establish connectivity and provide full access to DOORS for the major C2BMC facilities, ranges, other Government agencies, and support Contractors as requested by the Government. The Contractor shall provide technical assistance and information to support a Government Configuration Control Board.

#### **4.6 Analysis and Assessments**

The Contractor shall perform analyses supporting the BMDSS Build D and S8.2 capability evolution of the C2BMC Element addressing areas such as spiral content and growth planning, design trade-offs, algorithm development/effectiveness, capability specification, and performance prediction and assessment. This analysis shall demonstrate that the requirements allocated to C2BMC S8.2 are feasible and sufficient to achieve the desired performance within mandated latencies and allow for ease of implementing future enhancements or updates per the Modular Open Systems Approach (MOSA). The Contractor shall support the Integrated Master Assessment Plan (IMAP) planning, development, and execution.

##### **4.6.1 Analysis Report**

The Contractor shall develop and deliver detailed Analysis Report IAW DI-SESS-81785 (CDRL-A021) for C2BMC and Concurrent Test, Training and Operations (CTTO) Training System capabilities as required by the requisite task order statements of work.

#### **4.7 Technical Performance Measurement (TPM)**

The Contractor shall prepare and update the TPM Management Plan IAW DI-MCCR-80700 (CDRL-A019) and IAW DI-MISC-80508B TPM Baseline. If a change to the current baseline

is identified, the Contractor shall assess/update the TPM baseline and TPM Management Plan to reflect the change, which may include hardware and software upgrades.

#### **4.8 Program Report Database (PRD)**

The Contractor shall collect and track all Program-wide Program Reports originating from supported test events, exercises, end-users, and affiliated incremental developments and make available via the searchable repository.

#### **4.9 System Engineering Management Plan (SEMP)**

The Contractor shall prepare an Architecture and Systems Engineering Management Plan (ASEMP) IAW DI-SESS-81785 (CDRL-A020). The C2BMC ASEMP shall be consistent with the MDA System Engineering Management Plan DOC-3280.AA-SE-PLAN-Rev 1.0, 4 April 2011 (and updates as of 1 June 2011).

#### **4.10 System Integration Assessments and Special Studies**

As directed by the Government, the Contractor shall conduct integration assessments, special studies, and support activities to determine the impact of changes in assessed threats, missions, and unexpected BMDS tests results to C2BMC performance as specified in the CBS. Assessments include C2BMC Element and subsystem performance, requirements, interfaces and interoperability. Assessment reports shall be prepared IAW DI-SESS-81785 (CDRL-A021).

#### **4.11 Engineering Verification and Validation**

The Contractor shall support Component and Element verification and validation activities on Government approved and representative testbed hardware and software, models and simulation, including tools developed by the Contractor for successful conduct of the C2BMC program. The Contractor shall develop Analysis Method Papers describing the approach, analytical methods used, and Modeling & Simulation (M&S) selected for satisfying Verification and Validation (V&V) of the selected requirements. The Contractor shall define, document, and maintain the confidence level of the TPM and formal specification quantification analysis.

##### **4.11.1 Spiral Capability Verification Plan (SCVP)**

The Contractor shall prepare the SCVP IAW DI-MSSM-81751 (CDRL-A022). The SCVP shall be consistent with the C2BMC Spiral Capability Verification Plan.

##### **4.11.2 Spiral Capability Assessment Report (SCAR)**

The Contractor shall prepare a SCAR IAW DI-MISC-80508B. The SCAR shall be consistent with C2BMC Spiral Capability Assessment Report format.

#### **4.12 C2BMC Modeling and Simulation (M&S)**

The Contractor shall refine and use a combination of Government Furnished Equipment/Government Furnished Information (GFE/GFI) and Contractor-developed Modeling and Simulation (M&S) tools. The tools shall be used to verify and validate design and implementation concepts for every unit, as appropriate, of the subsystem and functionality therein to ensure performance requirements such as utilization, loss, latencies



and all other behavioral specifications are satisfied. In those cases where M&S tools need to be developed, the Contractor shall ensure they are compatible with or an extension of existing GFE M&S tools. The Contractor shall work closely with the MDA M&S Directorate and the BMDS elements to maximize the use of Government-sponsored M&S development efforts to support C2BMC Element development activities and to minimize cost. The Contractor shall collect, define, and track BMDS modeling and simulation capabilities and requirements consistent with the Spiral capabilities and the need to support C2BMC spiral development, integration, test and training. The Contractor shall perform software design, coding, and unit testing to develop the BMDS C2BMC Model (BCM) to provide high fidelity C2BMC functionality such that the model can be used with the Discrete Event Simulation (DESIm) or BMDS Digital Simulation Architecture (DSA) (whichever is required) for C2BMC performance evaluations, analysis activities, test event predictive analysis and system post-flight reconstruction (SPFR) participation and support. The Contractor shall use the results of ground tests that provide Critical Engagement Condition (CEC) Key Test Points (KTPs) useful for model validation. The Contractor shall prepare a description of the BCM to include functionality, high level algorithm logic descriptions, interface(s) with the DSA and DESIm architecture, and any capability limitations IAW DI-IPSC-81441A (CDRL-A029). The Contractor shall provide the DoD Information Assurance Certification and Accreditation Process (DIACAP) artifacts/documentation to support any certification required to interconnect BCM with MDA Digital Simulation Architecture. All software executables, source code, tool sets, libraries, licensing provisions and documentation for each increment shall be provided to the Government in accordance with the C2BMC contract technical data and computer software rights clauses.

#### **4.13 C2BMC Algorithm Engineering**

The Contractor shall participate in the Government's IPT process to ensure proper establishment, documentation and control of the algorithm baseline, critical methods, reference implementations, algorithm system engineering documents and reports, and architectures. This includes participation in a Cross-Product Team (CPT).

##### **4.13.1 C2BMC Algorithm Documentation, Reference Implementation, and Software**

The Contractor shall develop and deliver system engineering documentation to describe the C2BMC algorithms to include algorithm logic description, reference implementation, and critical methods for each C2BMC critical algorithm IAW DI-MISC-80711A/T and DI-IPSC-81435A/T (CDRL-A011). This documentation shall be consistent with the BMDSS. The Contractor shall prepare all source software and object code and associated data/documentation and deliver IAW DI-MCCR-80700 (CDRL-A044). The Contractor provided documentation shall provide insight into software, data, and deliverables. This information shall include all supporting Software Development Folder artifacts. Supporting documentation shall fully and accurately describe the delivered software source code and executables, and its associated requirements baseline and test reports.

#### **4.14 Element Effectiveness Performance Assessment**

The Contractor shall demonstrate the effectiveness of the C2BMC Element and Components against the threats and scenarios specified by the Government. Threat documentation

supporting the assessment shall contain threat characteristics and required engineering data IAW DI-MISC-80508B, the current BMDS threat documents, and Defense Intelligence Agency (DIA) threat assessment documents.

#### **4.15 C2BMC Element Interoperability**

The Contractor shall implement C2BMC S8.2 Element and the C2BMC S8.2 Element shall be interoperable with current and future elements as specified in the BMDSS. The C2BMC Element shall be interoperable to external BMD systems, including allies, as defined in the C2BMC System to External Systems Interface Specification (IFS). The Contractor shall provide technical and analytical support to MDA, BMDS, Joint Service, exercises, international exercises, demonstrations, selective data sharing and other interoperability/integration activities. The Contractor shall provide inputs to support Interoperability & Supportability (I&S) Certification of the C2BMC Net Ready-Key Performance Parameter (NR-KPP) IAW with Service, Joint Staff, and Office of the Secretary of Defense (OSD) guidance. The Contractor shall develop and deliver C2BMC element interoperability assessment reports IAW DI-MISC-80508B.

#### **4.16 Labs, Models, Simulations, and Testbeds Maintenance**

##### **4.16.1.1 Testing Activities at Product Integration Laboratories (PIL)**

The Contractor shall support product integration laboratories in conducting integration and testing.

##### **4.16.1.2 Models, Simulations, Testbeds, and Associated Software**

The Contractor shall develop and maintain models, simulations, testbeds, and associated software required to perform Contractor engineering analyses and tests. The Contractor shall deliver models, simulations, testbeds, and associated software to the Government simulation and Hardware-in-the-Loop (HWIL) facilities to include, but are not limited to, the Element and Component testbeds, Independent Verification and Validation (IV&V), and Imaging Infrared Simulation System (I2RSS) IAW DI-MCCR-80700 to ensure the Element configuration representation. The Contractor shall prepare all source software and object code and associated data/documentation and deliver IAW DI-MCCR-80700 (CDRL-A029). The Contractor provided documentation shall provide insight into software, data, and deliverables. This information shall include all supporting SDF artifacts. Supporting documentation shall fully and accurately describe the delivered software source code and executables, and its associated requirements baseline and test reports. The Contractor shall coordinate with other MDA Contractors and organizations for models and simulations required for C2BMC testing. The Contractor shall test all externally provided model and simulation updates to ensure that the updates perform sufficiently for use for C2BMC testing prior to deploying to the Contractor's development integration and verification testing labs.

#### **4.17 Software Engineering**

The Contractor shall implement and document a software development process that complies with the IEEE 12207 Software Life Cycle Processes, and consistent with the MDA Assurance Provisions (MDA-QS-001-MAP-Rev A).

##### **4.17.1 Software Development Plan (SDP)**

The Contractor shall support software development and operations and sustainment as described in the SDP IAW DI-MCCR-80700 and DI-IPSC-81427A/T (CDRL-A030). Software development planning shall be consistent with PL-DV-0001 the C2BMC Development Integrated Product Team SDP. The Government will require signature authority on SDP and all major revisions.

###### **4.17.1.1 Software Safety**

The Contractor shall, as part of software development effort, identify software safety critical functions. These shall be coordinated with and approved by the Government in writing. Software testing for safety critical software must be identified, and agreed to by the Government in writing. AR 385-17 and MAP shall be a source of guidelines for software development with regards to safety implementation.

###### **4.17.1.2 Software Quality Inspection Points**

The Contractor shall identify software quality inspection points, as part of the software development effort that will allow for Government verification and approval of software deliveries. These deliveries include every software component or troubleshooting procedures. Regression testing for critical functions and safety critical software must be identified, and agreed to by the Government in writing.

##### **4.17.2 Software Integration and Test Documentation**

The Contractor shall develop and implement a Software Integration and Test Documentation IAW the C2BMC Integration and Test Plan to identify the necessary test cycles to verify and qualify the software updates to the C2BMC Element which shall be consistent with DI-IPSC-81438A/T and DI-IPSC-81439A/T (CDRL-A061). The Contractor shall provide their Integration and Test Plan to the Government for review and approval in writing. The Contractor shall prepare an Acceptance Plan, acceptance test procedures, and final reports of results (CDRL-A022).

##### **4.17.3 Software Transition Planning**

The Contractor shall transition the software development resources to the maintenance organization as described in the Transition Plan (TP) IAW DI-IPSC-81429A (CDRL-A034). The TP shall identify the migration path for the software, Commercial off-the-Shelf (COTS), C2BMC Planner, and supporting software and data for the development and test environments consistent with the C2BMC Integrated Logistics Support Plan (ILSP). The TP shall describe plans to migrate tools to a single, common toolset.

###### **4.17.3.1 C2BMC Planner Transition Plan**

The Contractor shall develop, prepare, maintain and deliver a C2BMC Planner Transition Plan IAW DI-IPSC-81429A (CDRL-A033) to transition the C2BMC

Planner software and operational BMD plans at each fielding location, as applicable, from Spiral 6.4 to Spiral 8.2.

#### **4.17.4 Software Installation Planning**

The Contractor shall develop and implement a Software Installation Plan (SIP) for installation and training at user sites IAW DI-IPSC-81428A (CDRL-A035). Software installation planning shall be consistent with the C2BMC System Activation Plan.

#### **4.17.5 Software Maintenance Planning**

The Contractor shall implement the software maintenance processes as described in the Software Maintenance Plan (SMP) IAW DI-MCCR-80700 (CDRL-A036). The SMP is the organizational document for all Post-Deployment Software Support (PDSS) maintenance activities. Suppliers (Prime and Subcontractor) who maintain software products (whether performed internally or externally to an organization) shall comply with the SMP.

#### **4.17.6 Control and Management of Software Processes**

The Contractor shall perform all development and maintenance of software and test environments in a Software Configuration Management (SCM) environment IAW PL-PM-0003 the C2BMC Configuration Management Plan (CMP). The appropriate Contractor Configuration Control Board (CCB) shall review, prioritize, and maintain all updates to software, test environments and documentation. Contractor Software Quality Assurance (SQA) IAW PL-IT-0001 shall monitor and audit maintenance process steps to ensure that product quality and integrity of baselines and documents are maintained. Both the Government and Contractor Quality Assurance representative shall be notified of software quality reviews throughout all phases of development and testing. The Government shall be invited to all software quality reviews.

##### **4.17.6.1 Software Data / Supporting Information**

The Contractor shall prepare all source software and object code and associated data/documentation and deliver IAW DI-MCCR-80700 (CDRL-A044). The Contractor provided documentation shall provide insight into software, data, and deliverables. This information shall include all supporting SDF artifacts.

Supporting documentation shall fully and accurately describe the delivered software source code and executables, and its associated requirements baseline and test reports.

##### **4.17.6.2 Software Release Schedules**

The Government will approve in writing and control release schedules for installation of software and firmware to address program-wide needs and concerns, and to maintain system-level capability. The routine update process shall include both Problem Report (PR) solutions and any new functionality IAW PL-AL-0001 the C2BMC Architecture and Systems Engineering Management Plan.

##### **4.17.6.3 Software Metrics**

The Contractor shall provide software metrics for all software and firmware products and they will be captured IAW PL-PM-0007 the C2BMC Quantitative Management Plan. The Contractor shall retain and dispose of the records generated by this plan IAW the PL-PM-0005 C2BMC Data Management plan and the PR-PM-0059 C2BMC Records Management Procedure (CDRL-A037). The Contractor shall advise the Government of changes in software measurement parameters. The Contractor shall collect and report metrics to address five areas of the software program: schedule and progress, growth and stability, funding and resources, product quality, and technical maturity and risks and shall be consistent with the program life-cycle phase. The Government and the Contractor shall mutually agree on the software metrics.

#### **4.17.7 Software Problem Review, Prioritization, and Solution Implementation**

The Contractor shall partner with the Government to prepare, review, and prioritize all software Problem Reports (PRs) submitted to the Program Report Database (PRD) and Software Change Report (SCR) in preparation for executing Task Orders. The Contractor shall host periodic meetings with the user to discuss field problems and PR solutions. The Contractor shall design, develop, integrate, and test solutions to identified PRs and SCRs, and deliver software updates IAW DI-MCCR-80700. The Contractor shall synchronize new functionality updates with software problem solutions.

##### **4.17.7.1 Software Change Report (SCR) Tracking System**

The Contractor shall prepare an SCR tracking system IAW PL-AS-0001 and PL-DV-0001. The tracking system shall fully and accurately track all software changes as defined in the Configuration Management Plan (CMP). The Contractor shall update the tracking system to include the corrective action taken to resolve the issue. The Contractor shall provide unlimited Government access to the SCR tracking system from a Government accessible site.

##### **4.17.7.2 Program Report Database (PRD) with Software Problem Reports (PRs)**

The web-based, dynamically interactive PRD shall link all software PRs to the Software Change Report (SCR) Tracking System to synchronize reported software problems with associated SCRs. The Contractor shall update the PRD to include the corrective action taken to resolve the software issue. All suppliers who maintain software products (whether performed internally or externally to an organization) shall provide information to maintain the PRD. The Government will have read access to the PRD from a Government accessible site.

#### **4.17.8 Post-Deployment Software Support (PDSS) Maintenance Activities**

The Contractor shall perform PDSS maintenance activities IAW with the SMP. Contractor Software Quality Assurance (SQA) audits shall be performed to ensure that all required information is provided and acceptable for use during maintenance. Audit reports shall be provided quarterly or upon request IAW DI-MISC-80508B (CDRL-A039). The Contractor shall review the results with the Government upon request.

#### **4.17.9 Software Prototyping**

The Contractor shall provide software prototyping. The prototype shall have fidelity that allows the design complexity and interface of the eventual product to be evaluated against the software requirements. Prototyping shall be accomplished IAW PL-DV-0001 Appendix A.

#### **4.17.10 C2BMC Planner Hosting**

C2BMC includes a missile defense design C2BMC Planner that provides Blue Force Validation of BMDS element models, external interfaces with the Army's Air & Missile Defense Workstation (AMDWS) and the Army's Integrated Air and Missile Defense Battle Command System (IBCS), Modernized Integrated Database (MIDB), Navy's Maritime IAMD Planning System (MIPS), and C2BMC services to load C2BMC plans into GEM. The Contractor shall provide a minimum set of hardware/software system requirements to host the C2BMC Planner software.

#### **4.17.11 Software Test Environments**

C2BMC development environments shall be a functional representative of those used in test and operations. These environments and associated configurations shall be under SCM control. All software and firmware shall be released through the Software Development Library as defined in the CMP. Changes shall be IAW Spiral Capability Verification and Validation Plan.

##### **4.17.11.1 Access and Support to Independent Verification and Validation (IV&V) Agent**

Under the Government's direction, the Contractor shall provide requested data and support to the IV&V agents. Activities will include technical interchange meetings, and support providing data documentation and results for any element or system level tests conducted.

#### **4.17.12 Open Architecture**

The Contractor shall define, document, and follow a Modular Open Systems Approach (MOSA) for using modular design, and standards-based interfaces for the C2BMC. The Contractor shall obtain Government approval in writing regarding the use of any proprietary products prior to utilization.

##### **4.17.12.1 Software Reuse**

The Contractor shall plan, establish, manage, control, and monitor the software reuse program IAW IEEE 12207 and to systematically exploit reuse opportunities.

##### **4.17.12.2 Commercial Off The Shelf/Non-Development Items (COTS/NDI)**

If a vendor no longer supports the product versions used in the C2BMC environments, the Contractor shall, with Government concurrence, provide a technical assessment of risks involving unsupported product usage, and shall provide assessment of transition to upgrades with resulting retest and installation impacts. Each site shall provide input to the SMP for addressing changes to the environment.

#### **4.18 Configuration Management (CM)**

The Contractor shall develop, implement and maintain a program level CM Program. The Contractor shall update the C2BMC CMP PL-PM-0003 IAW DI-CMAN-80858B (CDRL-A041) to reflect how the program manages the hardware and software configuration items produced under this SOW. The Contractor shall define, develop and maintain the program-level CM system, including policies, board structures, processes, tools and procedures. The CMP shall also be updated as applicable to document the implementation of standards in accordance with the MDA Assurance Provision (MAP). The Contractor shall conduct CM IAW the C2MBC CMP, as updated. The Contractor shall review the plan annually with MDA and update it as necessary. CM requirements shall be flowed down to the Subcontractors and suppliers. The Contractor shall confirm that the Subcontractor and suppliers are in compliance with the CMP, as applicable, through the review and approval of their CM plans.

##### **4.18.1 Configuration Identification and Documentation**

The configuration identification for the C2BMC Element shall be as identified in the Functional Baseline, Allocated Baseline, and Product Baseline. The prime Contractor shall assign Government issued document/part numbers and Commercial and Government Entity (CAGE) codes for all C2BMC peculiar product definition documentation (specifications, drawings, parts lists, version description documents, etc.) for major items, critical items, components, etc., to be provisioned for re-procurement and/or spare/repair parts. The Contractor shall use Metric (System International) units, for all elements of new design and maximize the use of metric units in selecting/modifying existing designs consistent with current industry standards.

##### **4.18.1.1 Functional Baseline and Allocate Baseline Documentation**

The Contractor shall prepare the Functional Baseline and Allocated Baseline documents baselined by the Government at contract award. The System C2BMC Spiral Specifications (CBS) shall be prepared and delivered DI-SDMP-81465A (CDRL-A015). Interface Control Drawing documentation shall be prepared IAW DI-CMAN-81248A (CDRL-A013). Software Description Documentation shall be prepared and delivered IAW DI-MISC-80711A/T, DI-IPSC-81435A/T, DI-IPSC-81436A/T, DI-IPSC-81437A/T, DI-IPSC-81438A/T, DI-IPSC-81439A/T, DI-MISC-80508B, and DI-MCCR-80700 (CDRL A011), and Software Data and Documentation shall be prepared and updated IAW DI-MCCR-80700 (CDRL-A044).

##### **4.18.1.2 Product Baseline Documentation**

Product performance specifications, engineering drawings, part lists, process specification, material specifications, and computer software configuration documentation shall be prepared IAW DI-SDMP-81465A (CDRL-A045) and DI-SESS-81000D (CDRL-A045) to define the Product Baseline. The Contractor shall prepare requests for nomenclature IAW DI-CMAN-81254A (CDRL-A048) for all major end items that are to be type-classified.

##### **4.18.1.3 Breakout Item(s)/Spare Parts Documentation**

The Contractor shall develop product performance specifications and/or product drawings for all replacement assemblies and spare parts. At the discretion of the Government, the Contractor shall deliver the Product Baseline documentation/software for selected major end items, assemblies, and spare parts. (CDRL-A013)

#### **4.18.2 Configuration Change Control**

Specifications under Government change control at contract award, that are changes or variances to documents under Government control, shall be implemented only after Government approval of modifications to specification documents, prepared IAW DI-CMAN-80639C, or Requests for Deviation prepared IAW DI-CMAN-80640C (CDRL-A048), or Requests for Waiver prepared IAW DI SESS-81732 (CDRL-A048).

#### **4.18.3 Configuration Status Accounting**

The Contractor shall prepare a status accounting database that shall provide identification, status, and traceability for all technical and cost/schedule program documentation supporting Spiral delivery. The documentation shall be made available via an online data repository.

#### **4.18.4 Configuration Reviews and Audits**

The Contractor shall provide for and support to a S8.2 Government Functional Configuration Audit, to verify that the design meets or exceeds all Element performance requirements as reflected in the Functional Baseline and Allocated Baseline.

#### **4.18.5 Data Management**

The Contractor shall maintain the Program-level Data Management (DM) system as defined in the approved C2BMC Data Management Plan. The Contractor shall manage C2BMC data including collection, storage, management, preparation, distribution and disposition of product and program data items. This effort addresses unclassified and classified data received and generated on the program as well as securing and controlling access to and release of that data.

The Contractor shall manage a program library and confirm that access to library content and indices by all members of Contractor and the Government is available, upon request. The library accommodates both paper and electronic data.

The Contractor shall control access to data items stored in the library in accordance with the C2BMC DM Plan. The Contractor shall maintain a Data Accession List for Government access to data.

The Contractor shall review and manage documents to confirm that common formatting, correct marking and professional appearance of all generated briefings, CDRL items and other prepared and/or submitted documents are correct.



#### **4.18.6 C2BMC Element Configuration Database**

The Contractor shall prepare a C2BMC Element Configuration Database that fully and accurately tracks all software, hardware, firmware, and DoD Information Technology Standards Registry (DISR) Information Technology standards by version and major end item serial number, mission data files and profiles that correlate to each theater, geographical location, and test facilities. The Contractor shall post this database to the online data repository. The Contractor shall ensure traceability to the hardware and software baseline for all fielded C2BMC equipment.

#### **4.18.7 BMDS Core Standards Compliance**

The Contractor shall assess their compliance with BMDS Core Standards IAW MDA Directive 4122.01, Dec 2010, or any subsequent updates.

#### **4.19 Information Assurance (IA)**

Using established System Security Engineering processes, the Contractor shall implement security measures incorporating the security requirements of, but not limited to, the following documents:

- DoD5200.1-R Information Security Program Regulation
- NSTISSAM TEMPEST/1-92
- NSTISSI 7001
- NSTISSAM 2-95
- NSTISSP 11
- CNSS Advisory Memorandum TEMPEST 01-02
- Information Assurance, DoDD 8500.01E Information Assurance (IA)
- DoDI 8500.2 Information Assurance (IA) Implementation
- DoDI 8510.01 Information Assurance Certification & Accreditation Process
- NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations
- CJCSI 6510-01 Information Assurance (IA) and Computer Network Defense (CND)
- CJCSI 6211.02c, Defense Information Systems Network (DISN) Policy and Responsibilities
- DoDD O-8530.1 Computer network defense
- DoD 8570.01-M, Information Assurance Workforce Improvement Program.

The Contractor shall prepare:

- Threat and Vulnerability Analysis IAW DI-MISC-80841 (CDRL-A051)
- System Security Concept IAW DI-MISC-80840 (CDRL-A052)
- Communication Security (COMSEC) Material Control Guide IAW DI-MCCR-80340 (CDRL-A053)

The Contractor shall provide documents and engineering solutions in a level of quality to obtain Interim Authority to Test (IATT), Interim Authority to Operate (IATO), and optimally Authority to Operate (ATO) accreditation decisions.

#### **4.19.1 IA Program Management**

The Contractor shall conduct IA Program Management in accordance with best commercial practices. The Contractor shall incorporate security concepts provided by the current version of the NIST SP 800-100, Information Security Handbook: A Guide for Managers and Security Technical Implementation Guides (STIGS) Best Practices Security Checklist as applicable to the C2BMC program processes.

#### **4.19.2 Management Practices**

The Contractor shall conduct Program Management in accordance with best industry practices. The Contractor shall develop a Security Engineering Management Plan that identifies the security engineering processes to the Government IA Lead.

##### **4.19.2.1 Interfaces**

The Contractor shall manage security-engineering efforts within the C2BMC program that supports MDA/BC's requirements. The Contractor shall interface with various elements within the MDA to include the office of the Designated Accreditation Authority (DAA), the office of Security and Intelligence, the C2BMC Program Office. The Contractor shall interface with external agencies dealing with IA direction and guidance, such as the National Security Agency (NSA), the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), the National Institute of Science and Technology (NIST), and other cooperating agencies/Services/contractors. The contractor shall ensure internal IA processes and activities are aligned with MDA and DoD processes.

##### **4.19.2.2 Planning**

The Contractor shall plan and execute a security-engineering program and shall document that planning in a Program Planning Schedule in accordance with the C2BMC program processes.

##### **4.19.2.3 Reporting**

The Contractor shall report the status of the IA program on a regular basis in a contractor developed format. The report will include the status of all Controls Validation Testing (CVT) (conducted and/or planned), the current Plan of Actions, and Milestones (POA&M), and current Accreditation approvals with the expiration dates.

The Contractor shall support weekly meetings with MDA/BC IA. This reporting will contain the status of specific support events such as Certification and Accreditation status for all C2BMC operating locations and network connection.

##### **4.19.2.4 IA Engineering**

The Contractor shall conduct Security Engineering in accordance with best security practices and guidelines provided in the DoDI 8500.2, IATF, DISA Security Technical Implementation Guides (STIGS), and NIST. The Contractor shall support the mission of the C2BMC by interfacing with internal Integrated Product Teams (IPTs) to ensure IA Security requirements (i.e., IA Controls) have been identified and properly integrated into the system design. The Contractor shall support Government

related engineering meetings, forums, boards and activities, including the C2BMC IA Engineering Board (IAEB) to ensure IA is adequately and properly integrated into the system design as required by DoD and MDA requirements. The Contractor shall report on the progress of engineering efforts in the monthly progress report.

#### **4.19.2.5 Architecture Updates**

The Contractor shall sustain a current IA architecture. The IA architecture in concert with the internal processes and interfaces with various IPTs will ensure the C2BMC system architecture includes all IA Controls: required in Section 2.0 of this SOW and support the Architecture Working Group as described in Section 4.1 of this SOW. The Contractor shall update the IA architectures in the form of architecture drawings.

#### **4.19.2.6 Design Updates**

The Contractor shall conduct IA design updates to ensure that IA architectures, approved by the C2BMC Information Assurance Engineering Board (IAEB) and applicable MDA/BC Program Management, will be updated, and sustained through this period of performance. The contractor shall work closely with all IPTs to ensure all IA controls as identified in the approved architecture and the references in SOW Section 2.0 are maintained in the system design. The contractor shall also update the Security Configuration Guide and Functional Architecture Design Documents (FADDs) as required after system updates.

#### **4.19.2.7 Change Management**

The Contractor shall conduct change management in accordance with the Contractor Configuration Management (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 Certification and Accreditation (C&A) documentation. The Contractor shall use internal CM processes and the IAEB to evaluate IA related changes. The Contractor shall plan for and execute procedures for the development and execution of changes due to events defined by the Government.

#### **4.19.2.8 Change Proposals**

The Contractor shall support the Configuration Management process for IA related changes and develop changes to system documentation used to support design, development, test and Certification and Accreditation (C&A).

#### **4.19.2.9 Test Support**

The Contractor shall interface with internal IPTs, Government organizations and boards to support system test and engineering aspects of test activities. The Contractor shall develop all Certification and Accreditation (C&A) artifacts necessary to support accreditations in support of the C2BMC and BMDS-level test events and activities.

#### **4.19.2.10 Notice and Event Analysis and Response**

The Contractor shall interface with required C2BMC boards to respond to IA security alerts, IA vulnerabilities announcements and policy updates from DoD, MDA, NIST, and STIGS effecting C2BMC. The Contractor shall conduct IA security tests to

determine where IA vulnerabilities exist and develop mitigation techniques and strategies to eliminate or reduce the effects of known and new threats. The Contractor shall analyze IA vulnerabilities and coordinate solutions following C2BMC program processes. The Contractor shall analyze, test, and/or develop an automated patch management system to remotely manage, release, and update: Information Assurance Vulnerability Alert (IAVA) patches, hardware, software and virus updates. The automated patch management system will manage the Original Equipment Manufacturer (OEM) updates that enhance the overall process of evaluating, approving, developing, testing, and implementing changes due to the identification of vulnerabilities and OEM weaknesses and implement at a selected site as a Proof of Concept in the Spiral 8.2 timeframe. The Contractor shall report on the progress of Contractor efforts in the monthly progress report. Full implementation of this remotely managed capability within the C2BMC Element will occur in Spiral 8.2.

#### **4.19.3 DoD Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (DIP)**

The Contractor shall develop a DIP using the approved DoD template per major spiral in accordance with the guidelines provided in DoDI 8510.01. The DIP will clearly identify all IA controls listed in DoDI 8500.2 for a Mission Assurance Capability (MAC) I, Classified system and cross-reference these controls to all system test procedures, including STIGs, SRRs, and internally developed Certification, Test and Evaluation (CT&E) test procedures. The DIP will augment the IA artifact package required by DoDI 8510.01 for C&A.

#### **4.19.4 IA Risk Management**

The Contractor shall conduct IA risk management in accordance with the Contractor internal risk program and risk approaches as agreed with MDA/BC IA. The Contractor shall supply monthly IA risk charts for the C2BMC Executive Risk Board Briefing. The Contractor shall integrate the risk management effort throughout the C2BMC IA engineering effort and process. The Contractor shall use the internal IPTs and Government boards to assist in the IA risk assessment process.

#### **4.19.5 IA Technology Refresh**

The Contractor shall conduct analyses and research into emerging technologies and prototypes, under the auspices of the C2BMC IAEB, to enhance C2BMC security posture. This research shall be augmented by interfacing with: other Government agencies and departments that are conducting like research and developing ways to mitigate known and future IA vulnerabilities (risk). These risks can be found in, but not limited to,

(b)(3):10 U.S.C. § 130

The Contractor shall use the C2BMC's IAEB as a forum to discuss, review, plan for, and seek approval to procure for further research, on any/all future technology items. The Contractor shall procure the appropriate hardware to support security prototypes as directed by the Government.

#### **4.19.6 DIACAP Artifact Development**

The Contractor shall assemble artifacts and prepare documentation in accordance with DoDI 8510.01 (DIACAP) to support C&A for all C2BMC operating locations. The Contractor shall ensure that all documents prepared during this effort are properly marked in accordance with the BMDS Security Classification Guide, MDA security guidelines, and applicable DoD security directives to ensure proper classification of the data recorded in each document. The Contractor shall ensure the appropriate templates and formats as required by DoD and MDA are used for the document preparation process. The Contractor shall ensure that the accuracy of each document is verified by coordinating with internal IPTs and having formal reviews with the appropriate IPTs. After internal reviews, the Contractor shall staff the DIACAP Artifacts through the MDA/BC Information Assurance Manager (IAM), the C2BMC IAEB, and C2BMC Program Manager for review and approval prior to being staffed to the DAA to support the DAA's C&A decisions.

#### **4.19.7 Plan of Action and Milestones (POA&Ms) Development**

The Contractor shall develop POA&Ms, input data into the Defense Information System Agency (DISA) Vulnerability Management System (VMS) website/database, generate reports and produce artifacts needed to support the MDA DAA's C&A decisions and, as required, to address remaining security vulnerabilities (risk). This includes performing vulnerability assessments using the DISA STIG compliance scripts/RPMs and Gold Disk to evaluate monthly IA releases. These IA artifacts and VMS inputs will address issues detected during CT&E testing conducted by the Contractor, the DAA's independent Controls Validation Testing (CVT) teams, the Staff Assistance Visits (SAVs), the DoD Inspector General (IG) audits, Blue/Red Teams reviews, DISA validation requirements and Interface Tests and others as directed. The Contractor shall transition from legacy IA POA&Ms to the Vulnerability Management System tool. The Contractor shall develop IA POA&Ms within VMS to support C2BMC sites, and generate them monthly. The Contractor shall maintain an internal database, as required, as a means to verify and reconcile the accuracy of the VMS, and for IA program management activities. The Contractor shall provide monthly IA lockdowns for C2BMC systems to stay current with Information Assurance Vulnerability Alerts (IAVA) from Joint Task Force-Global Network Operations (JTF-GNO).

#### **4.19.8 Certification Test and Evaluation (CT&E) Test Development**

The Contractor shall perform CT&E following C2BMC program processes. The Contractor shall develop CT&E test procedures, conduct CT&E tests, correct IA deficiencies as agreed upon at the C2BMC Program Software Control Board. The Contractor shall provide test results and reflect IA issue disposition in the VMS and contractor database as required to support trend analysis and C&A activities for each component within the C2BMC at COCOM and fielded sites. The C2BMC CT&E test procedures shall encompass applicable DISA Security Technical Implementation Guides (STIGs) and CVT test tools (e.g., Nessus, NMAP use of the tools is within available resources, etc., as specified by the Government in their CVT Test Plan) as necessary to identify IA issues. The Contractor shall implement corrective actions, as early as possible prior to the Software Shipping Readiness Review (SRR). The Contractor shall assess the areas of testing coverage afforded by the DISA and CVT test tools and prepare

a list of CT&E test procedures needed to provide complete testing coverage of all IA controls within the C2BMC. The Contractor shall vet CT&E test procedures through the C2BMC IAEB.

#### **4.19.8.1 IA Operations**

The Contractor shall provide operational security support to COCOM and fielded sites. The Contractor shall coordinate this support by interfacing with all internal IPTs, Government offices, and boards to insure that IA is properly addressed in TOs, Notice and Event Handling, Site Assistance Visits (SAVs), CVT testing, Computer Network Defense (CND), and system modifications required to support all missile test activities.

#### **4.19.8.2 Site Assistance Visits Support**

The Contractor shall support combined SAV/CVT activities conducted by the Government to assess the IA posture at all COCOM and fielded sites. This support will consist of providing Visit Request coordination, scheduling time with the Site-specific Information Assurance Officer (IAO) as well as privileged Users and IA support personnel for IA Control Checklists, quick look reports, trend analysis, POA&M development/modification, documentation reviews, and coordination with the site lead personnel to insure non-interference with system operations.

#### **4.19.8.3 Controls Validation Testing Support**

The Contractor shall support both combined and standalone SAV and Controls Validation Testing (CVT) activities. The Contractor's support shall consist of providing IA technical personnel to be available during applicable CVT activities, completing the Site Survey Questionnaire (SSQ), supporting Technical Interchange Meetings, verifying asset management schedules, arranging for administrative support. The Contractor shall, coordinate with relevant parties to ensure that the testing will not interfere with system operations, providing applicable documentation required by the CVT team in order to accomplish required testing in a timely manner, and reviewing and evaluating CVT test results for the Government to determine the validity and applicability to C2BMC. The Contractor shall support DISA STIG and the Government/CVT special purpose IA vulnerabilities assessment tool testing. This support shall encompass reviewing and evaluating CVT test results for the Government to determine the validity and applicability to C2BMC. All outstanding vulnerabilities will be checked and reported in the POA&M and/or VMS as applicable.

#### **4.19.8.4 External IA Assessments and Joint Interface Testing Support**

The Contractor shall support a maximum of two annual external IA Vulnerability Assessments, such as DoD Inspector General Team, National Security Association (NSA) Blue Team, United States Air Force (USAF) Blue Teams, or other independent DoD or MDA sponsored IA Reviews. In addition, the Contractor shall support one (BMDS Element-to-BMDS Element) Joint Interface Test (JIT) per year as requested.

#### **4.19.9 Information Assurance Officer Support**

The Contractor shall provide personnel to fulfill the duties and responsibilities of an Information Assurance Officer (IAO) in accordance with DoDI 8500.01. C2BMC Suites located at COCOM Sites and C2BMC operating locations specified by the Government shall have an IAO designated by the C2BMC IAM (in writing) to oversee the IA and CND activities for their assigned Area of Responsibility (AOR) as per the C2BMC Network Defense Appendix to the BNOSC-C CONOPS. In the case of the BNOSC-C located at the Missile Defense Integrated Operations Center (MDIOC), an IAO will be assigned to coordinate Notice and Event Handling and other Government directed IA actions prior to release to the site IAOs for action.

The IAO shall develop, maintain, and utilize nominal security standard operating procedures as agreed to with the Government. IAOs shall develop site-specific IA Incident Response Procedures (IRPs), Disaster Response, Continuity of Operations Procedures (DR/COOPs), (in partnership with the both the CUBE, BNOSC-C, JFCC-IMD, and C2BMC IAO) and provide (and document) IRP and DR/COOP training to C2BMC Users annually.

IAOs at C2BMC operating locations shall plan and develop operationally realistic IRP and DR/COOP scenarios, and conduct site-level IRP and DR/COOP exercises as follows: 1) a minimum of one table-top IRP exercise and one table DR/COOP exercise per year, and 2) conduct a minimum of two actual DR/COOP exercises per year as approved by the C2BMC IAM. C2BMC IAOs shall document IRP and DR/COOP events, and exercises, capture lessons learned, conduct IRP and DR/COOP retraining as required when training deficiencies are noted, and shall provide Quick-Look Reports as soon as possible from any actual/exercise event, updated as required, to the BNOSC-C and CUBE and shall provide comprehensive After-Action Reports as required after applicable exercise/actual events to the BNOSC-C, CUBE, and C2BMC IAM via secure communications.

#### **4.19.10 Information Assurance Training**

The Contractor shall insure that personnel working directly or indirectly in the IA field shall be trained IAW DoD 8570.1. The Contractor shall develop a training plan IAW DoD 8570.1 and will list applicable personnel with their work assignments and levels of responsibilities, IAW the guidelines of DoD 8570.1.

#### **4.19.11 Information Assurance Vulnerability Management (IAVM)**

The Contractor shall develop and maintain an IAVM Plan IAW DI-MISC-80508B (CDRL-A055) for C2BMC hardware and software.

#### **4.19.12 Computer Network Defense**

The Contractor shall provide Network Defenders to support the BMDS Network Operations and Security Center (BNOSC) as appointed by the C2BMC Information Assurance Manager (IAM). The Contractor shall develop, maintain, and utilize standard operating procedures required to support Network Defender capabilities as agreed to with the Government. The Contractor shall provide an Information Assurance Officer (IAO)

to support the BNOSC-C as appointed by the C2BMC IAM and defined in the IAO appointment letter.

#### **4.19.13 Security and Architecture Integration**

The Contractor shall ensure that the software and infrastructure architecture design process(es) includes evaluation by IA engineers to identify and mitigate or correct potential security shortcomings or vulnerabilities prior to detail design and development. This approach will reduce the risk of inherent security flaws that could require expensive re-engineering.

### **4.20 Security Engineering**

The Contractor shall incorporate security features into the C2BMC Element designs using established System Security Engineering processes IAW DoD 5200.1-M, "Acquisition Systems Protection Program," and MIL-HDBK-1785, "System Security Engineering Program Management Requirements," and DoDI 8500.2 "Information Assurance (IA) Implementation."

#### **4.20.1 Security Management**

The Contractor shall provide security management on the program that will ensure the protection of both classified and unclassified Program information. This shall be done to ensure that all program personnel, MDA-designated Federally Funded Research and Development Centers (FFRDCs); Assistance and Advisory Services (A&AS); and MDA staff members are able to access Contractor information and facilities as required and permitted. The Contractor shall follow DoD and MDA security policies and guidance to ensure the protection of the classified areas and information.

#### **4.20.2 Security Requirements Traceability Matrix**

The Contractor shall develop a Security Requirements Traceability Matrix (SRTM) per major spiral IAW the guidelines provided in DoD 8510.1-M. This SRTM will clearly identify associated IA controls listed in DoD 8500.2 for a Mission Assurance Capability (MAC) 1 system and cross reference these controls to applicable system test procedures, including references to Security Technical Implementation Guides (STIGS), Shipping Readiness Review (SRRs), and internally developed Certification, Test and Evaluation (CT&E) test procedures. The SRTM will augment the IA artifact package required by DoD 8510.1-M for Certification and Accreditation (C&A). The Contractor shall provide security management on the program that will ensure the protection of both classified and unclassified Program information. The Contractor shall ensure that all personnel under their responsibility, are cleared to the appropriate level, up to Top Secret/Sensitive Compartmented Information (TS/SCI) as required, and are able to access Contractor information and facilities as required and permitted.

#### **4.20.3 IA Design Activities**

The Contractor shall conduct IA design activities to ensure that IA architectures, approved by the C2BMC Information Assurance Engineering Board (IAEB), and applicable C2BMC Program Management Office, are incorporated into the C2BMC system design. The Contractor shall work closely with internal IPTs and Government IA



engineering offices and boards to ensure that IA controls listed in DoD 8500.2 for a MAC I system are included or mitigated in the system design. The Contractor shall also develop a Security Configuration Guide and Functional Architecture Design Documents (FADDs).

#### **4.20.4 IA Engineering**

The Contractor shall conduct IA Engineering in accordance with best internal practices and those guidelines provided in the DoD 8500.2, Information Assurance Technical Framework (IATF), DISA Security Technical Implementation Guides (STIGS) and NIST Special Publication 800-27A Engineering Principles for Information Security Technology, Revision A. The Contractor shall support the mission of the C2BMC by interfacing with internal Integrated Product Teams (IPTs) to insure that IA Security requirements (i.e., IA Controls) have been identified and properly integrated into the system design. The Contractor shall support Government related engineering meetings, forums, boards and activities as required, including the C2BMC IA Engineering Board (IAEB) to insure that IA is adequately and properly integrated into the system design. The Contractor shall report on the progress of engineering efforts in the monthly progress report.

#### **4.20.5 IA Architecture Development**

The Contractor shall conduct IA architecture development in concert with the internal processes and interfaces with various IPTs to insure that the C2BMC system architecture includes or mitigates IA Controls. All IA controls shall be met or mitigated to the Government's satisfaction in order to obtain accreditation of the MAC-I Classified system. Within the Architecture, the Contractor shall include the placement and functionality of the BMDS Network Operations and Security Center – C2BMC (BNOSC-C). The Contractor shall determine the needs of Network Defenders in the BNOSC-C with respect to security operations, operational software tools, and computing hardware requirements in order to support the Computer Network Defense (CND) function. The Contractor shall ensure compliance with an approved BNOSC Concept of Operations (CONOP) and operational security requirements set forth in a Network Defense and System Security Appendix to the BNOSC-C Continuity of Operations (CONOPS) under separate cover. The Contractor shall document these IA architectures in the form of architecture drawings.

#### **4.20.6 IA Risk Management**

The Contractor shall conduct IA risk management in accordance with the Contractor internal risk program, the BMDS risk management program and pertinent guidance provided in DoD 8500.2, the IATF, and the guidance provided in NIST Special Publications 800-30, 800-100, and 800-27A. The Contractor shall integrate the risk management effort throughout the IA engineering effort. The Contractor shall use the internal IPTs and Government boards to assist in the IA risk assessment process and report Contractor progress on a monthly basis.

#### **4.20.7 IA Vulnerabilities Mitigation**

The Contractor shall conduct analyses and research into emerging technologies and prototypes, under the auspices of the C2BMC IAEB, to enhance C2BMC security posture. This research shall be augmented by interfacing with other Government agencies and departments that are conducting like research and development into ways to mitigate known and future IA vulnerabilities found in Information Technology (IT) products such as firewalls, routers, switches, operating systems, cross-domain-solution (CDS) products, Internet Protocol (IP) encryption, CND capabilities, cryptographic equipments; such as Key Generators (KGs) and High Assurance Internet Protocol Equipment (HAIZE) devices. The Contractor shall use the C2BMC's IAEB as a forum to discuss, review, plan for and seek approval to procure for further research future technology items. The Contractor shall provide the appropriate hardware to support security prototypes.

#### **4.20.8 IA Configuration Management**

The Contractor shall support the Configuration Management process for IA related changes and develop changes to system documentation used to support design, development, test and Certification and Accreditation (C&A). The Contractor shall ensure that applicable modifications affecting IA functionality are brought before internal Contractor boards, the joint C2BMC IAEB and the BMDS level boards prior to formal release.

#### **4.20.9 C2BMC Operations Security (OPSEC) Plan**

The Contractor shall implement and maintain a C2BMC Operations Security (OPSEC) Plan IAW DI-MGMT-80934C (CDRL-A056).

#### **4.20.10 Anti-Tamper (AT) Techniques**

The Contractor shall analyze AT techniques for the C2BMC Element design to delay exploitation and unauthorized disclosure of critical technologies, IAW the Core Standards. The Contractor shall apply anti-tamper techniques to C2BMC Critical Program Information. The Contractor shall use the systems engineering approach to identify relevant threats and their associated vulnerabilities, identify available AT measures for consideration, and perform trades to determine the best approach for protecting the individual critical technologies.

The Contractor shall review trade study inputs and results with the Government upon request.

#### **4.20.11 Certification and Accreditation**

The Contractor shall complete, maintain, and provide DoD Information and Assurance Certification and Accreditation Process (DIACAP) documents per the Government direction, and engineering solutions of quality to obtain Interim Authority to Test (IATT), Interim Authority to Operate (IATO), and optimally Authority to Operate (ATO) accreditation decisions IAW DoDI 8510.01 and the MDA Plan 8500.2-P MDA Information Assurance Program Plan (CDRL-A057).

#### **4.20.12 Network Connections**

The Contractor shall support and maintain the program Secret Internet Protocol Router Network (SIPRNet) connection to include maintaining a Web-based data repository, controlling access to the Web site and coordinating Memorandum of Agreement(s) (MOA[s]) for access to external SIPRNet sites. The Contractor shall oversee the operation of links between the Contractor facilities and the classified MDANet and Secret Internet Protocol Router Network (SIPRNet) (where applicable) since the preponderance of classified processing will be at the Secret System High classification level. The Contractor shall provide the capability to communicate over secure communications between Contractor and Government sites.

The Contractor shall:

- a. Participate in Government led security working group meetings to identify specific Contractor security requirements and propose security solutions for the protection of MDA data and technologies.
- b. Maintain an expanded Standard Practice and Procedure (SPP) document that includes site-specific protection strategies for MDA Critical Program Information and Critical Research and Technology used by the prime or subcontractor.
- c. Participate in the development of Counterintelligence Support Plans to identify critical information (Critical Program Information or Critical Research and Technology) and the foreign intelligence collection threat to this information at the prime and subcontractor locations.
- d. Meet certification and accreditation requirements established by Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and the MDA Designated Accrediting Authority (DAA) before connection to the MDA Classified Network (MDACNet) or SIPRNet environments. The Government will provide any additional monitoring resources or equipment required to support Computer Network Defense (CND) activities.
- e. Maintain Public Key Infrastructure (PKI) capability compatible with MDA C2BMC systems.

#### **4.20.13 Reporting**

The Contractor shall report the status of the IA program on a monthly basis in a Contractor developed format. This reporting will be augmented by weekly reports on the status of specific support events such as: C&A status for applicable C2BMC operating locations and network connection approvals, as required by the MDA DAA, Joint Staff, Combatant Commanders (COCOM), Services, or Agencies for the C2BMC Element, including specified communication systems necessary for C2BMC operations such as SIPRNet, Non-Classified Internet Protocol Router Network (NIPRNet), Defense Red Switch Network (DRSN), and Passive Taps (examples). Additionally, the Contractor shall provide for reporting on those areas of deficiencies noted during the conduct of the management of the IA section of this contract. These deficiencies shall include personnel, hardware, software and fiscal needs and shall be reported to the Government in order for

the Government to assess the deficiencies and make appropriate adjustments to the contract when necessary to implement mitigations.

#### **4.21 Engineering and Technical Services for Production and Deployment Support**

The Contractor shall provide engineering and technical services to produce C2BMC systems and sustain deployed C2BMC configurations up to and including Spiral 8.2. The Contractor shall integrate and coordinate all technical requirements for production and field support with the requirements for C2BMC development.

#### **4.22 Facility and Data Access**

The Contractor shall provide facility access to the Government and its representatives. The Contractor shall provide access to all data and documentation necessary for Government insight into the hardware and software development, maintenance, and products.

The Contractor shall establish and maintain a development environment at their own facility. The Contractor shall obtain Government approval in writing prior to acquisition of any equipment, in order to avoid procurement of equipment/software that may be available as Government-Furnished Equipment (GFE) or may be employed at Government facilities without impacting Contractor schedules. The Contractor shall also establish the capability to accomplish electronic (internet) transactions and development between the C2BMC development team located at the Contractor's own facilities and Government facilities.

The Contractor shall deliver the following CDRL IAW Defense Priorities and Allocations System (DPAS): Government Furnished Property (GFP) and Contractor Acquired Property (CAP) Listing(A091); and Final Property Identification Listing DI-MGMT-80443 (A092).

#### **4.23 Future Activities Transition**

The Contractor shall provide technical support services that support Government activities to enhance or add additional capability beyond the specified C2BMC Spiral 8.2, to assure uninterrupted follow-on Contractor assumed responsibilities. Technical support services include, but are not limited to participation in Government sponsored Integrated Product Teams (IPTs), technical interchange meetings, and system integration and test activities for future C2BMC spiral development and operational activities.

##### **4.23.1 Advanced Concepts & Technology Evaluation**

The Contractor shall develop proposed modification to the S8.2 Architecture and Requirements, upon written Government direction, to experiment with Advanced Concepts & Technology including but not limited to: Airborne Infrared (ABIR)/Precision Tracking Space System (PTSS) Integration, Overhead Persistent Infrared (OPIR) Tasking, Aegis Engage-on-Remote, Infrared/Radio Frequency (IR/RF) Integrated Discrimination, Weapon Peer-to-Peer (P2P) Engagement Coordination (e.g., simultaneous requests for support, distributed weighted engagement schema, shoot-shoot, shoot-look-shoot) and monitoring of P2P engagement coordination for the purpose of exercising management by exception.

#### **4.23.2 Long Lead Architecture, Algorithm, Experimentation, and Engineering Support**

The Contractor shall support Long Lead efforts for System of Systems architecture and engineering, C2BMC architecture and engineering, interfaces assessment, algorithm and critical methods generation, future studies, experimentation, future capabilities, roadmap generation, and other activities as requested by the Government.

##### **4.23.2.1 X-Lab Activities**

The Contractor shall leverage the experimentation infrastructure in X-Lab and the interface developed at the Space Based Infrared Sensors (SBIRS) Mission Control Station Backup (MCSB) Operations Migration Capability (OMC) for research and development capability for Spiral 8.2 based development and characterization. The X-Lab and SBIRS OMC shall be used for the characterization of engineering releases. To accomplish this work; the X-Lab shall receive direction and engineering releases from the DEV IPT.

### **5.0 SYSTEM TEST AND EVALUATION**

#### **5.1 System Testing**

The Contractor shall support the BMDS Integrated Master Test Plan (IMTP) planning, development, and execution. The Contractor shall provide the Level of Support as required based on the current IMTP, as provided by the Government, for Flight and Ground Tests. The Contractor shall collect C2BMC event data to assess C2BMC performance, Critical Engagement Conditions (CECs) and Empirical Measurement Events (EMEs). The Contractor shall perform analysis of the collected data to support Program Change Board (PCB) fielding decisions.

##### **5.1.1 System Test Planning**

The Contractor shall support test planning associated with BMDS system test events that include C2BMC. The Contractor shall provide support to relevant system test planning, which includes support to test architecture design and definition, requirements, Test Objectives Memorandums (TOMs) (review of both system and C2BMC test objectives), goals scorecard, scenario/test case design, CECs/EMEs, and the Government objectives suitable to address C2BMC system performance, interface verification, and model validation.

##### **5.1.2 System Test Coordination of Planning, Execution, and Analysis**

The Contractor shall plan, execute, and provide the analysis and reports for the five phases of testing as defined in the BMDS Test Policy including, but not limited to, development of test objectives, data requirements, test configurations, integration and analysis plans, test planning documentation, and supporting schedules. The Contractor shall participate and provide inputs into the C2BMC Test Objectives Working Group (CTOWG), Network IPT Review Panel (NIRP), Weekly Analysis Status Update (WAS-UP), Program Engineering Review Board (PERB), Synchronization of Program Execution Activity Roundtable (SPEAR) and Internal Configuration Control Board (ICCB), as appropriate. The Contractor shall provide Capability Thread analysis and

traceability mapping to TOM objectives, test scenarios, and BMDS Test Incident Report (BTIRS) for each test.

### **5.1.3 Technical Support to Testing**

The Contractor shall participate in Government test planning, evaluation and analysis, and reporting activities. The Contractor shall provide data and analysis as required to support each test event. This is to include pre-mission data resulting from models and simulations to support HWIL tests and flight tests. Necessary information shall be provided for the Government to host and interpret the data. The Contractor shall provide detailed plans and procedures for the test program IAW DI-NDTI-80603A and DI-MISC-80652 (CDRL-A001). The Contractor shall conduct pre-mission analysis for testing where C2BMC is a participant, as outlined in the IMTP. The Contractor shall deliver the pre-mission analysis in briefing format. The Contractor shall provide Test Reports for all BMDS Flight and Ground tests where C2BMC participates except for Level 1 support events; including a section that describes how applicable CECs and EMEs were satisfied or not satisfied. The Contractor shall support the BMDS test objective and planning activities within MDA.

### **5.1.4 Test Readiness Reviews (TRR)**

For Contractor-conducted tests, the Contractor shall conduct readiness reviews prior to each Spiral in accordance with the IMS. Prior to TRR, the Contractor shall prepare Interim Authority to Test (IATT) and Interim Authority to Operate (IATO) documentation. For Government-conducted tests, the Contractor shall provide technical support to Government readiness reviews.

### **5.1.5 Ground Test Conduct, Range Simulation, and Analysis**

The Contractor shall participate in BMDS ground test planning, execution, and reporting activities. The Contractor shall provide technical support in the areas of test planning, trajectory analysis, interoperability, and integration.

### **5.1.6 Data for Joint Analysis Team (JAT)**

The Contractor shall provide technical support to the JAT process for pre-mission and post-mission activities on all ground and flight tests where a JAT or Government led analysis activity is convened.

## **5.2 Sensor Interface Operations**

The Contractor shall provide operation and sustainment support to deployed C2BMC Communication Interface Nodes associated with BMDS Sensors.

## **5.3 Contractor Support to Government Ground Testing**

The Contractor shall participate in and provide system test and component Subject Matter Experts to support the development of detailed test plans and procedures for Government Ground Testing. Government testing includes, but is not limited to, qualification tests, safety tests, and environmental tests. The Contractor shall assist in test planning and coordination, test execution, data collection and analysis, and test reporting/reviews. The Contractor shall provide and coordinate maintenance and logistics support of equipment under test.

#### **5.4 Contractor Support to Government Flight Testing**

The Contractor shall participate in and provide system test and component Subject Matter Experts to support the development of detailed test plans and procedures for Government Flight Testing. Government testing includes, but is not limited to, qualification tests, safety tests, and environmental tests. The Contractor shall assist in test planning and coordination, test execution, data collection and analysis, and test reporting/reviews. The Contractor shall provide and coordinate maintenance and logistics support of equipment under test.

#### **5.5 BMDS Test Incident Reports (BTIRs)**

The Contractor shall participate in and provide technical support as directed to the development, assessment, tracking, and resolution of BTIRs as they are generated in relation to the various ground and flight test events.

### **6.0 QUALITY, SAFETY, AND MISSION ASSURANCE (QSMA)**

#### **6.1 Quality Assurance (QA)**

The Contractor shall develop and implement a QA program that integrates QA requirements into the design, development, and test of all C2BMC Element hardware and software. The Contractor quality management program shall be compliant with the requirements of ISO 9001. The Prime Contractor shall conduct audits and perform analyses to ensure the Prime Contractor's major subcontractors and vendors are compliant with the QA program. The Contractor's quality program shall ensure that all inspections/tests in the contract requirements that are contained in the Contractor's development, design and test planning and implementation documents are being performed. The Contractor shall flow down appropriate requirements to Subcontractors and suppliers to ensure overall compliance to the contract. The Contractor shall support Government quality audits and evaluations IAW the MAP. Any and all QA Plans required to meet the entire section 6.1 shall be included in the Data Accession List.

##### **6.1.1 Quality Assurance Program Plan (QAPP)**

The Contractor shall implement and maintain a QAPP. The QAPP shall be prepared and submitted IAW DI-QCIC-81794 (CDRL-A058). The QAPP shall also provide for support of the monthly C2BMC Quality Assurance/Mission Assurance Working Group (QA/MAWG). The Contractor shall set up a video-teleconference, provide agenda, and participate in monthly QA/MAWGs. The Contractor shall provide facilities for, set up and participate in a minimum of two QA/MAWGs per year in Huntsville, AL. The Contractor shall provide full access to their program audit database or equivalent, used on the Program.

##### **6.1.2 Missile Defense Agency Assurance Provision (MAP) and Parts, Materials, and Processes Mission Assurance Plan (PMAP)**

The Contractor shall develop, implement, and maintain a Quality, Safety and Mission Assurance (QSMA) program in compliance with the requirements of the Missile Defense Agency Assurance Provisions (MAP) and Missile Defense Agency Parts, Material, and Processes Mission Assurance Plan (PMAP), design standards, clauses, and provisions

identified in this contract. The Contractor's internal C2BMC documents/media, including quality documents, internal design standards, procedures, processes, build papers, test documentation, and internal specifications form a part of the QSMA program and are considered contractual obligations. The Contractor shall flow-down applicable MAP, PMAP and command media requirements to applicable lower-tier suppliers based on complexity, criticality and risk. Flow-down to lower-tier suppliers should follow the same process as the flow-down for any standard. When a conflict arises between the Contractor's media and the MAP or PMAP, the MAP or PMAP takes precedence.

### **6.1.3 Mission Assurance Implementation**

The Contractor shall implement the MAP and PMAP requirements and document their compliance in a document approved by the Government. Should there be any deviation to the MAP, the Contractor shall develop a compliance to MAP criteria matrix (Requirements Applicability Matrix (RAM)) DI-MISC-80508B (CDRL-A086) describing the Contractors approach for each MAP/PMAP requirement including the implementation methodology and rationale for exceptions. All deviations from the MAP must be approved by the Government.

#### **6.1.3.1 Material Review Board (MRB) Authority**

IAW MDA Directors Memorandum dated 23 Oct 09, the Prime Contractor shall retain MRB authority and not delegate to subcontractors.

#### **6.1.3.2 Maintenance and Availability of Quality Records**

The Contractor shall maintain quality records, documents, processes, and procedures IAW applicable quality systems. The Contractor shall facilitate Causal Analysis to identify and eliminate defects and reduce variation. The Contractor shall monitor health and status of the program and report to the Government, Program Director and other Stakeholders through formal defined reviews and status reporting. Records shall be made available to the Government upon request.

#### **6.1.3.3 Shipping Readiness and Deployment**

The Contractor shall conduct a hardware Shipping Readiness Review (SRR) prior to shipping hardware to a site. The Contractor shall conduct a software ship readiness review prior to sending C2BMC applications software to the field for each major spiral delivery. The software SRR is conducted to ensure the readiness of the spiral software for delivery to the operational sites. The Government shall have final approval of SRR and delivery of hardware and software to the field.

#### **6.1.3.4 System Certification**

The Contractor shall establish and maintain a process that furnishes to the Government a Certification Data Package (CDP), signed by the Chief Engineer, Program Manager, and the Contractor Quality Lead, or equivalent, at the conclusion of any Pre Shipment Review and prior to all test events. Certification Data Packages are critical components of the Test Event Certification (one of several instruments used to record how BMDS tests are planned and executed) which are used to document and track the locked down as-built hardware and software configuration of



a particular asset or group of assets participating in a BMDS test event. Each CDP is held as the baseline configuration for the associated asset(s), and changes are incorporated only after they have been approved thru the Program Change Board (PCB), Test Configuration Working Group (TCWG), or current Test Phase Office of Primary Responsibility (OPR).

The Contractor shall compile and provide a CDP IAW DI-MISC-80508B (CDRL-A060). The CDP will provide the identification and traceability of all hardware and software and its documentation relative to each IMTP / C2BMC Event Scheduling Board (CESB) directed event unique System Under Test (SUT). This requirement applies for both flight and ground tests as determined and updated by the IMTP and CESB. The Contractor shall include top level hardware drawing(s), parts list(s) with serial numbers, software segment listings with version numbers, and individual applicable TPs for each SUT. The Contractor shall make all information documented in each event unique CDP available at the request of the Government and provide technical assistance / facilitator for the Government pre-event SUT audits at the various locations that may be participating in any particular event. All CDPs shall be considered quality records and a copy of each shall be stored in the SDFs.

#### **6.1.3.5 Software Qualification**

The Contractor shall perform Software Qualification IAW the Integration and Test Plan (CDRL-A061). A requalification decision, including supporting rationale shall be approved and retained for record, for each major software delivery proposed for approval and use in the operational BMDS system. These requalification decisions shall be available to the Government for review upon request. Test reports shall be delivered as agreed upon per test event.

The Contractor shall establish and maintain a process that will furnish to the Government a CDP IAW DI-MISC-80508B (CDRL-A060) signed by the Chief Engineer, Program Manager, and the Contractor Quality Lead, or equivalent, for each delivery of software intended for use in the BMDS Operational system.

#### **6.1.4 C2BMC Element Hardware and Software Acceptance**

The Contractor shall develop an Acceptance Test Plan (ATP) for all major hardware and software deliverables. The ATP shall be prepared IAW DI-QCIC-80553A and DI-MISC-80711A/T (CDRL-A032).

#### **6.1.5 Software Quality Assurance (SQA)**

The Contractor shall conduct a SQA program for C2BMC software development consistent with the C2BMC Quality Assurance Program Plan and the Integration Test Plan. The Contractor shall prepare a monthly status report of SQA activities IAW DI-MISC-80508B (CDRL-A063).

#### **6.1.6 Quality Metrics**

The Contractor shall capture metrics in accordance with MDA Directive 4245.01. These shall be submitted IAW MDA Directive 4245.01, MDA-QS-001-MAP Rev A, MDA

Assurance Provision (MAP), DI-MISC-80508B, PL-PM-0007, PL-PM-0005, and PR-PM-0059 (CDRL-A037).

## **6.2 Reliability, Availability, & Maintainability Program**

The Contractor shall implement and maintain a Reliability, Availability and Maintainability (RAM) Program Plan to predict whether or not the C2BMC system will meet RAM Specifications. The Reliability, Availability and Maintainability Program Plan shall be prepared and submitted IAW DI-SESS-81613 (CDRL-A065). The Contractor RAM Program shall support the BMDS Joint Reliability & Maintainability Evaluation Team (JRMET), Data Scoring Board (DSB) and Operational Test Agency. (Annex XX)

### **6.2.1 Joint Reliability and Maintainability Evaluation Team (JRMET)**

The Contractor shall establish a Reliability, Availability, and Maintainability (RAM) effort to support the Joint Reliability and Maintainability Evaluation Team (JRMET) process and Failure Reporting Analysis and Corrective Action System (FRACAS), based upon data analysis obtained during operational periods to improve reliability and maintainability for C2BMC, through collection and analysis of failure data, indentifying causes, frequency, corrective actions and obsolescence. This process should include reporting by location and nodal operations, to include communications and networks. The Contractor shall establish a process to review maintenance actions and identify maintenance False Indications of Failure/Malfunction (“bad actors”) and cost drivers to improve RAM and reduce support costs in accordance with RAM guidelines for the equipment hardware, software, and/or firmware covered by this SOW. The Contractor shall perform RAM analysis on C2BMC systems (hardware, software, and firmware); and use a data collection system, predictive tools, and methods to identify areas of improvements, and document the results of this effort. Reference documents include the MDA JRMET Charter dated January 2007 and any future revisions. (Annex XX)

### **6.2.2 C2BMC Reliability, Availability, and Maintainability Modeling**

The Contractor shall incorporate Operational Trouble Ticket data into the RAM model. The Contractor shall use model results and analyze the data as a basis to make recommendations to improve the C2BMC reliability and maintainability. The Contractor shall conduct Reliability, Availability, and Maintainability (RAM) modeling to predict whether or not the C2BMC system will meet the RAM Specifications. The RAM model shall provide estimates for Mean Time Between Failures (MTBF), Mean Time to Restore (MTTR), Mission Reliability, and Availability, and Failure Reporting Analysis and Corrective Action System.

### **6.2.3 Failure Reporting Analysis and Corrective Action System (FRACAS)**

The Contractor shall utilize a closed-loop Corrective Action System FRACAS during the build-up/manufacture of all development hardware/software, and during all testing to include field-testing, to address all Contractor and Subcontractor hardware/software failures and BTIRs. All Contractor and Subcontractor level supporting test data and analyses shall be included as part of FRACAS. The Contractor shall establish a Failure Review Board (FRB) to determine root cause and ensure timely corrective action for critical failures. The Contractor shall provide summary status for each and all

hardware/software failures that may affect testing, attesting to proper root cause, corrective action, and closure during Phase 3 of the testing process. (Annex XX)

#### **6.2.4 Failure Modes Effects and Criticality Analysis (FMECA)**

The Contractor shall prepare or update a bottoms-up FMECA concurrently with the design effort on applicable newly designed or modified hardware. Functional FMECAs shall be performed on Government Furnished Equipment (GFE) and Commercial off-the-Shelf (COTS) equipment. Reliability Critical Items (RCIs) shall be identified by the FMECA and procedures for controlling and testing RCIs shall be documented. The FMECA report shall be prepared IAW DI-ILSS-81495. (Annex XX)

#### **6.2.5 Element Fault Detection, Fault Isolation**

The Contractor shall prepare Element fault detection, fault isolation analyses IAW DI-RELI-80255 (CDRL-A065) to ensure RAM requirements are achieved when new, modified, or redesigned hardware is incorporated into the design.

### **6.3 Parts, Material, and Processes**

The Contractor shall implement a program to control Parts Materials and Processes IAW the Government approved Parts, Materials, & Processes (PMP) plan.

#### **6.3.1 Counterfeit Part Avoidance/Mitigation**

Purchasing Electronic Parts shall be done IAW MDA Policy Memorandum 50, dated 29 Jun 09. Procurement of electronic piece parts from non-authorized/non-franchised independent distributors shall only occur when there is not an Original Equipment Manufacturer (OEM) or an OEM-authorized/franchised source available. Suppliers shall be assessed for a high likelihood of supplying reputable product, including prior performance and assessment audits. The Contractor shall notify the Government in all cases when a non-authorized independent distributor is required for procurement of electronic piece parts. This notification shall include documented evidence that an OEM-authorized/franchised source was not available and identification of testing performed to validate part authenticity. The Contractor shall request approval of all deviations from this policy from the Government IAW DI-CMAN-80640C (CDRL-A048).

#### **6.3.2 Parts Obsolescence**

The Contractor shall conduct an internal parts obsolescence program IAW the Government approved PMP Plan. The Contractor shall prepare a proactive process to address Obsolescence /Diminishing Manufacturing Sources (DMS) issues. The process shall include (a) a quarterly, Contractor-led Obsolescence Working Group (OWG) meeting; (b) a procedure to evaluate and respond to End of Life Notification; (c) DMS prediction techniques; (d) DMS resolutions and implementation techniques; and (e) A procedure to generate and track obsolescence cases.

##### **6.3.2.1 Obsolescence Identification**

The Contractor shall provide a quarterly Obsolescence Report to inform the Government of current and predicted DMS risk/obsolete parts, materials, or assemblies IAW DI-MISC-80508B. The Contractor shall notify the Government, if it

is determined that a part, material, or assembly required in the delivery of the system is unavailable due to Obsolescence/DMS issues within 30 days after identification. The Contractor shall identify the next higher assembly where obsolescence component issues occur, and define impacts to all applicable assemblies. The Contractor shall identify obsolete, in-house Special Test Equipment (STE).

#### **6.3.2.2 Obsolescence Mitigation Implementation**

The Contractor shall implement solutions to resolve/mitigate obsolescence issues.

### **6.3.3 Bill of Materials Management**

The Contractor shall develop and maintain procurement Bill of Materials (BOM) to cover hardware, software, maintenance and services required in support of program execution. The Contractor shall generate engineering drawings, when appropriate, to identify materiel requirements at a level of detail adequate for procurement. The Contractors shall baseline the BOM and manage changes in accordance with program configuration control procedures. The Contractor shall monitor new materiel requirements and identify when changes are required to BOM line items to meet baseline program requirements.

## **6.4 Safety Engineering**

The Contractor shall comply with all applicable local, state, federal, and Host Nation safety laws/regulations as well as the safety requirement of the Missile Defense Agency Assurance Provisions (MAP). The Contractor shall have effective policies and procedures in place to protect the life and well being of people (Contractor, Government, soldiers, and the public), and property and equipment.

### **6.4.1 System Safety**

The Contractor shall establish and maintain a safety program and shall ensure that safety considerations are integral parts of the system engineering efforts. The safety program shall address personnel and equipment concerns relative to the C2BMC life-cycle phases.

#### **6.4.1.1 Program Safety**

The Contractor shall develop a System Safety Program Plan (SSPP) per DI-SAFT-81626 (CDRL-A069). The SSPP shall address how the Contractor will implement a MIL-STD-882C compliant safety program. Specifically, the SSPP shall list the management structure, independent safety reporting chain, hazard tracking procedures, and analysis methods to be used in the development of the Safety Assessment Report (SAR) and Subsystem Hazard Analysis (SSHA), as appropriate. The SSPP shall list other safety analysis and safety deliverables which the Contractor anticipates or are required by this SOW. The SSPP shall specify how safety will be integrated into system design, software development, and testing processes. The SSPP shall provide for the C2BMC System Safety Working Group (SSWG), as well as support to the BMDS-level SSWG. The Contractor shall set up a video-teleconference, provide agenda, and participate in monthly C2BMC SSWGs. The Contractor shall provide facilities for, set up and participate in a minimum of two C2BMC SSWGs per year in Huntsville, AL. The Huntsville SSWGs should be in conjunction with the BMDS SSWG. The BMDS SSWG is the preferred method for

identifying safety critical interfaces; the Contractor shall document the safety critical interfaces identified by the SSWG in the appropriate ICD's. Safety critical interfaces are defined as those functions identified by the elements or by C2BMC as mitigations against a hazard, and which cross over the interface to/from C2BMC. Safety risks shall be identified for C2BMC life cycle phases, and shall be assessed by the Contractor through the use of hazard logs IAW categories in MIL-STD-882C and MDA memorandum, Updated Safety Risk Acceptance Authority, dated 7 May 2007. The Government safety office will use Contractor provided safety logs to prepare residual safety risk assessment and obtain appropriate acceptance IAW MDA policy.

#### **6.4.1.2 Safety Assessments & Analyses**

The Contractor shall develop a Safety Assessment Report (SAR) per DI-SAFT-80102B/DI-SAFT-80105B (CDRL-A070). The SAR shall document, among other items, safety critical software, safety critical interfaces, hazard controls and identify any non-compliances/variances with the BMS System Specification. The Contractor shall submit Hazard Logs as part of the SAR, and at the Government's request, populated in to the MiDAESS Web-based Hazard Tracking System. The Contractor shall prepare a safety requirements/ criticality analysis; a subsystem Safety Hazard Analysis (SSHA) DI-SAFT-80101B; element hazard analysis and safety assessment IAW MIL-STD-882C (CDRL-A071); DI-SAFT-80102B (CDRL-A071); and DI-SAFT-80106B (CDRL-A071), respectively.

#### **6.4.1.3 Review of Changes/Problems**

The Contractor shall review hardware and software changes/problems for safety impact and notify the Government of any impact to the level of safety IAW MIL-STD-882C.

#### **6.4.1.4 Safety Verification**

The Contractor shall define, support, and validate and verify requirements and design of safety critical hardware, software, and procedures IAW MIL-STD-882C. Validations and verifications shall be identified to the Government prior to implementation for concurrence. The requirements and appropriate validations and verifications necessary for safety critical hardware, software, and procedures shall be identified in the hazard logs in the Government provided Hazard Tracking System (HTS).

### **6.4.2 Safety and Occupational Health**

The Contractor shall develop, implement, and deliver an Environment, Safety, and Occupational Health (ESOH) program, IAW Contractor environmental, health, and safety standards and MDA-QS-001-MAP.

#### **6.4.2.1 Occupational Health and Safety**

The Contractor shall comply with federal (OSHA), state and local laws, regulations, and rules. Activities to support this include performing: operating and support hazard analysis and health hazard assessment IAW DI-SAFT-80106B (CDRL-A072) and the MAP. The Contractor shall maintain accurate accident and injury/illness records for

the C2BMC Element. For Contractor or Subcontractor work performed on Government installations, the Contractor shall notify DoD installation Commander, or designee, immediately (flash notification via telephone and/or email) of accidents, injuries, environmental illnesses, or other issues regarding compliance with regulations or policies.

The Contractor shall conduct accident investigations and provide documentation to the host installation and MDA's Quality and Safety Office, which will be provided to the Procurement Contracting Officer (PCO) or Contracting Officer's Representative/Contracting Officer's Technical Representative (COR/COTR) upon request. When requested, the Contractor shall conduct these investigations IAW MDA Manual 6055.02M, Safety Investigations and Reporting.

The Contractor shall support the development of the Programmatic Environmental, Safety & Health Evaluation (PESHE) as requested.

The Contractor shall comply with MDA Directive 6055.04, Work Time Restrictions for Safety and Mission Critical Personnel Supporting Tests and Critical Operations.

## **6.5 Environmental Management**

### **6.5.1 Environmental Laws**

The Contractor shall comply with all Host Nation (HN), Federal, State, and Local environmental laws, regulations, and policies, at Government and Contractor facilities. The Contractor shall manage the efforts under this contract so that C2BMC Element design, development, test, manufacturing, operation and disposal activities prevent, mitigate, or control adverse environmental impacts, including industrial pollution and hazardous wastes. The Contractor shall report environmental releases and/or incidents (including violations) IAW the Host Nation Agreement.

#### **6.5.1.1 Environmental Analysis Reporting**

The Contractor shall provide qualitative and quantitative data to support the required Government analyses related to environmental issues for new/relocated development, manufacturing, test or operational sites (that have not been previously analyzed or approved) under the provisions of the National Environmental Policy Act (NEPA).

## **7.0 SPIRAL OPERATIONS, SUSTAINMENT, AND SYSTEM DEPLOYMENT**

The Contractor shall operate and/or provide operational and sustainment support to the fielded U.S. and applicable International C2BMC operational hardware/software configurations, including COCOM C2BMC Suites, remote Enterprise Workstation (EWS) and web browser locations, planner laptops, the Distributed Training System (DTS) and Global Engagement Management (GEM) Suites to meet the Government's operational and test objectives.

### **7.1 Operations**

### **7.1.1 Operations and Maintenance**

The Contractor shall establish and maintain a maintenance planning program that addresses operations, operations support and sustainment to the fielded operational C2BMC Element and test assets including future site activations. Planning shall include identification of required/recommended spare parts and components and modules and Test Measurement and Diagnostic Equipment (TMDE) necessary to sustain the C2BMC Hardware/Software (HW/SW).

The Contractor shall provide operations and sustainment for fielded C2BMC equipment, back capability, Information Assurance and Communication Security (COMSEC) administration. The Operation & Sustainment (O&S) shall be on-site and the Contractor shall provide helpdesk and reach back capability. The Contractor shall maintain a surge capability to provide 24 hour a day operations and sustainment support for up to thirty days at a time, with a minimum of 72 hour pre-notification. All Operations and Maintenance personnel assigned to an active C2BMC operational location will be considered as Mission Essential/Emergency Essential.

NOTE: For Contractor personnel serving in an Area of Responsibility (AOR) that requires Technical Expert Status Accreditation (TESA) and in accordance with DoD Instruction 3020.37, "Continuation of Essential DOD Contractor Services during Crises," effective November 6, 1990, overseas positions supporting the Contingency Architecture Activation Team effort in Germany and Israel, and other overseas positions supporting MDA under this Contract, the Contracting Officer hereby designates the following positions/job functions as Emergency/Mission Essential:

1. EUCOM Operations and Sustainment Lead/Technical Expert (TE)
2. A&SE COCOM Site Engineer/TE
3. BNOSC Network Engineer/TE
4. MDA Information Assurance Officer/TE
5. Network Engineer, BMDS Communications Network/TE
6. Operations and Sustainment IPT Watch Stander/TE
7. Operations and Sustainment Gateway Operator/TE
8. Warfighter (WF) EUCOM Site Lead/SME/TE

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 Statement of Work. 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 DD-1172 and Common Access Card (CAC).

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.

### **7.1.2 C2BMC Asset Management**

The Contractor shall establish and maintain a C2BMC asset management function.

### **7.1.3 C2BMC Sensor Interface Operations & Maintenance**

The Contractor shall provide operations and sustainment support to C2BMC interface equipment and designated communication GFE, associated with BMDS sensors to meet the Governments operational, exercise, and test objectives, including all future node deployments.

### **7.1.4 C2BMC BMDS Network Operation & Security Center**

The Contractor shall provide Engineering, O&S, Network, and IA support to C2BMC prime mission network equipment located at the Missile Defense Integration and Operations Center (MDIOC) and monitor BMDS network equipment at all other operational sites, to include systems administration, network and Information Assurance/Computer Network Defense (IA/CND) security engineering support. The Contractor shall monitor operational networks 24 hours a day, 365 days per year basis, and provide outage reporting, network scheduling, metrics and management functions.

The Contractor shall support use of and modify as needed an automated common workflow process system, following the Information Technology Infrastructure Library (ITIL) model, as identified in the SOW or via trade study e.g. Gartner report. The Contractor shall use this system for all outage reporting, management of outages, Tasking Orders, incidents, implementation flows and monitoring of Information Assurance Vulnerability Alerts (IAVA's) and Information Assurance Vulnerability Bulletin/Information Assurance Vulnerability Management (IAVB/IAVM), Configuration Management and metrics where possible or applicable. System should be able to receive automated outage information from the Network Management System (NMS) or Intrusion Detection System (IDS). The Contractor shall support a common Configuration Management Database (CMDB) for all asset data and other artifacts as described in the ITIL best practices.

The common workflow process shall be integrated to the maximum extent possible with all C2BMC operational and developmental elements to include BMDS Computer Emergency Readiness Team (CERT), MDA CERT and Administrative/General Service (Admin/GENSER) workflow systems where Operations and Support can be integrated for maximum efficiency.

### **7.1.5 Site Lead**

The Contractor shall provide an O&S Site Lead for each location as directed by the Government. The O&S Site Lead will be capable of assuming the duties and responsibilities for each subordinate position on a temporary basis. The O&S Site Lead will be responsible for all aspects of C2BMC support, interfacing with other command representatives, maintain system readiness to the standard directed by the Government and preparing plans and procedures for the introduction of new or modified HW/SW into the site. The site lead shall interface and coordinate with the host installation or other representative as necessary to sustain C2BMC operations. Site lead will maintain all



records of equipment configurations, personnel qualifications and training and other records as required.

#### **7.1.6 C2BMC Control Center (CUBE)**

The Contractor shall provide 24 hours per day, 365 days per year C2BMC operations and maintenance Control Center (CUBE). The Contractor shall provide help desk and job control functions over all C2BMC fielded assets and establish and track metrics via the CUBE. The Contractor shall provide real world operations, test, and exercise support using the Cube as the central operations management entity.

#### **7.1.7 Test Support**

The Contractor shall provide 24 hours per day, 365 days per year C2BMC operations and maintenance support to tests and exercises as scheduled in the Integrated Master Test Plan.

### **7.2 Sustainment**

#### **7.2.1 Logistics**

The Contractor shall establish and maintain a comprehensive logistics program to provide support for existing and planned U.S and International C2BMC deployed operational hardware/software. The Contractor shall ensure that support considerations are addressed early and continuously in the HW/SW life cycle to ensure that the system can be cost-effectively supported through its life cycle, and that the infrastructure necessary to support initial fielding and operational support of the system are identified, developed and acquired in time to support the C2BMC program. The Contractor shall provide a Supportability Strategy IAW DI-ILSS-80095 and develop/update Site Specific Support Plans IAW DI-ILSS-80095.

##### **7.2.1.1 Maintenance Planning**

The Contractor shall structure the support program to align with the Government directed on site staffing requirements and C2BMC system operational readiness requirements.

##### **7.2.1.2 Supply Support Planning**

The Contractor shall institute and maintain a supply support program to ensure parts availability and accountability for all C2BMC equipment items, including spares and GFE. Modernization through spares may be addressed.

##### **7.2.1.3 Item Unique Identification (IUID) Requirements**

The Contractor shall establish and maintain an IUID programs to mark components, parts, and end items. The Contractor shall enter the IUID and required data elements into the IUID Registry. The Contractor shall update the IUID Registry for parts provided as GFE already having an IUID assigned.

##### **7.2.1.4 Support Equipment/Test Measurement and Diagnostic Equipment (SE/TMDE)**

The Contractor shall establish and maintain a SE/TMDE program.

**7.2.1.5 Packaging, Handling, Storage, and Transportation (PHST)**

The Contractor shall establish and maintain a packaging, handling, storage, and transportation program.

**7.2.1.6 Computer Resource Support Planning**

The Contractor shall establish and maintain a computer resources support program, to support the mission critical computer hardware and software assets necessary to operate or support the C2BMC system.

**7.2.1.7 Manpower and Personnel**

The Contractor shall establish a manpower and personnel program for identification of both Contractor and Government/military personnel required in support of C2BMC and associated systems, and equipment.

**7.2.1.8 Facilities**

The Contractor shall establish and maintain a facilities program that includes both Government and Contractor facilities planning.

**7.2.1.9 Design Interface**

The Contractor shall establish and maintain a design interface program. This program shall be an integrated program addressing systems engineering disciplines, Integrated Logistics Support (ILS) elements and other parameters required to design, support and maintain the C2BMC system.

**7.2.2 Sustaining Engineering**

**7.2.2.1 Technical Refresh**

The Contractor shall perform Technical Refresh as needed to ensure mission readiness for the operational system. This will include fielding of updated HW and SW as needed due to vanishing vendors, parts/support obsolescence, Government Industry Data Exchange Program (GIDEP) alerts, and metrics trends that indicate increased failures that may impact mission readiness.

**7.2.2.2 System Enhancements**

The Contractor shall upgrade the Regional Test Bed (RTB) at all locations, such that flight and ground tests can be conducted without interrupting BMDS Operations. The Contractor shall provide additional upgrades to the BMDS Network Operation and Security Center for RTB monitoring and management capabilities.

**7.2.3 Training, Training Media and Training Devices**

The Contractor shall establish and maintain a training program to develop, maintain, and conduct operator training for the operational C2BMC systems. The Contractor shall provide operations and sustainment support to C2BMC training devices hardware and

software including workstations, laptops, mobile training devices, and training suites. The program shall include curriculum identification and development, course conduct, identification of skills and personnel. The Contractor shall develop and maintain C2BMC training devices hardware and software. The Contractor shall support training for friends and allies.

#### **7.2.4 Technical Data**

The Contractor shall develop and deliver Training Material DI-ILSS-80872, Training Plan DI-ILSS-81070, Operator Manual DI-TMSS-80527B, and other technical documentation DI-CMAN-80776 to support operations and maintenance of C2BMC spirals including drawings, diagrams, instructions, technical manuals, DIACAP artifacts, and guides. Commercial format is acceptable and should include operation and maintenance of the Operator Workstation (OWS), EWS, Laptops, Web Browsers, and associated communication and processing equipment. Use of commercial technical data is authorized and should include system description and operation; normal and emergency procedures; cautions, notes, and warnings; and maintenance procedures (troubleshooting; remove, replace, operations check out procedures; preventative maintenance procedures; and an illustrated parts breakdown).

### **7.3 System Deployment**

#### **7.3.1 System Deployment and Site Activation**

The Contractor shall integrate site/system activation activities and collaborate with the appropriate Government organizations. The Contractor is responsible for building the overall site/system activation approach with the Government, performing specific hardware fielding and security engineering tasks, and providing status to MDA. The Contractor shall provide a Site Installation Plan IAW DI-MGMT-80033A.

##### **7.3.1.1 Fielding Engineering**

The Contractor shall perform system activation activities associated with the activation of new sites, and enhancement of existing sites. The Contractor shall provide initial engineering and CONOPS development leadership. The Contractor shall develop, provide and update site hardware drawings to document the specific site system configuration including hardware and network components that are relevant to the C2BMC system. The Contractor shall provide engineering support for C2BMC- Air Operations Center (AOC) Integration, as directed by the Government, and in association with the C2BMC-AOC Mutual Commitment Package (MCP, 6 Nov 08).

##### **7.3.1.2 System Activation Process**

The Contractor shall perform system activation activities, installation (fielding), checkout and activation of deployed C2BMC hardware and software. The scope of fielding engineering includes the planning and execution of all system activation activities related to installation, security engineering, and the removal.

##### **7.3.1.3 Fielding Activities**

The Contractor shall complete any remaining hardware installation activities required to field Spirals.

#### **7.3.1.4 Fielded Hardware Lists**

The Contractor shall update the CM baseline Automated Release Baseline Tracking System (ARBTS) database quarterly. ARBTS includes part number, serial number, model number, OEM, and nomenclature and identifies installed software (OEM, version, release, and support agreement data [date installed, support agreement start and expiration dates, etc.]), for each hardware component. The Contractor shall develop, provide, and update a list of in-stock inventory and a list of idle and excess equipment.

#### **7.3.1.5 Decommissioning & Disposal**

The Contractor shall establish an active program to continually monitor equipment, parts, hardware, software, and firmware to include Commercial Off-The-Shelf (COTS) and Government Off-The-Shelf (GOTS) for proper disposal.

### **8.0 WARFIGHTER INTEGRATION**

The Contractor shall assist the Government to establish and maintain a Warfighter support program that is integrated with O&S. The Warfighter support program shall include direct coordination with COCOMs and COCOM representatives at all levels. The Contractor shall have subject matter experts in support of Warfighter requirements. The Contractor shall develop and support demonstrations and other events.

#### **8.1 Wargames and Exercise Support**

The Contractor shall integrate and test C2BMC in exercises and provide candidate display concepts for Wargames to solicit Warfighter feedback on applicability to concepts, Doctrine, Tactics, Techniques and Procedures (DTTPs) and C2BMC suitability to prosecute combat operations.

#### **8.2 Friends and Allies Support**

The Contractor shall provide Warfighter / Subject Matter Expert (SME) support to friends and allies on C2BMC systems and associated equipments.

#### **8.3 Warfighter User System Modification Request**

The Contractor shall support the Government's Warfighter Involvement Process (WIP) and other Warfighter processes.

#### **8.4 Human Factors Engineering (HFE) Working Group**

The Contractor shall support the Human Factors Engineering (HFE) Working Group to assess product usability, suitability, and completeness and to identify new features/requirements that could be included in future versions of the C2BMC Suite. The Contractor shall develop and maintain the Display Description Document (DDD) IAW DI-MCCR-80700 (CDRL-A043).

## **9.0 BMDS COMMUNICATION & NETWORK DEVELOPMENT**

The Contractor shall support the development of a robust, end-to-end, high availability and survivable operational BMDS Communications Network (BCN) that will satisfy requirements to share information across the global BMDS consisting of multiple sensors, weapons systems and command and control nodes. This BCN connectivity between BMDS elements, Combatant Commanders (COCOMs), selective Host Nations (HN) and agencies is a force multiplier. C2BMC and the Contractor shall develop, field, and sustain an operational BCN that ensures that communications and networking are not the limiting factors in the fielding or operation of the BMDS.

(b)(3):10 U.S.C. § 130

### **9.1 Government Furnished Long-Haul Communication Services**

The Contractor shall use Government Furnished Services (GFS) for Long-Haul Communication Transport (LHCT). The contract design shall include GFS performance into the network performance design such that the GFS is included in overall network performance analysis (e.g., availability/reliability, packet loss rates, bit error rates, etc).

#### **9.1.1 Interface Control Specification**

The Contractor shall prepare, maintain, and submit an LHCT Interface Control Specification (ICS) for network requirements IAW DI-SESS-81314A (CDRL-A082). Requests for GFS LHCT will include the appropriate ICS reference. As a minimum the ICS shall include any Contractor requirements for:

- Availability
- Reliability
- Redundancy
- Diversity (Path/Equipment/Facility)
- Error rates tolerances (packet, bit error/bit error densities, etc)

Alternatively the Contractor may request only that performance meet the requirements identified in DISA Circular 310-175-9. In either case the Contractor shall warrant and be able to demonstrate that the GFS LHCT performance is satisfactory for the C2BMC to meet the allocated C2BMC network requirements as provided in the C2BMC Element Specification.

### **9.2 Network Development**

The Contractor shall develop the BCN as required by C2BMC for the Spiral 8.2; verify its configuration and performance through modeling and simulation in a laboratory environment before releasing it for higher level integration and testing; and support system integration and testing. The Contractor shall provide briefings, designs, test plans, test procedures, and test results for review and approval. The Contractor shall support development of Operations Task Links as appropriate to integrate C2BMC with GMD, Aegis BMD, Aegis Ashore, THAAD and Patriot, and others as appropriate. The Contractor shall develop a cyphertext core network, utilizing packet prioritization schemes and priority cueing. The Contractor shall develop an Internet Protocol Address Plan and deliver it IAW DI-SESS-81000D. The

Contractor shall develop a robust, fault tolerant, high performance network routing design and document the scheme. The Contractor shall provide an Out of Band (OOB) Network Management capability. In this construct OOB is defined as a separate network channel provided for Network Management, Security and remote access which is separate and potentially diverse from the Mission based network routes. The Contractor shall provide Element level connectivity to C2BMC and intra-C2BMC node connections IAW DI-SESS-81309A (CDRL-A084) including four functional areas of network development:

- a) BCN IP Core Network (NetCore): NetCore consists of the physical networks, network operating systems, Virtual Local Area Network (VLAN) structures, IP addresses, network protocols and applications required for delivering BMDS information
- b) BCN Link 16 Gateways: consist of COCOM Area of Responsibility (AOR) Air Defense System Integrators (ADSI) and MIL-STD-3011A Link 16 communications with BMDS Elements and Host Nation Interfaces
- c) BCN Network Security (NetSec): NetSec consists of systems and devices used by network operations security staff to manage the protection of BMDS mission data and to detect violations of information security policies
- d) BCN Network Management (NetMgmt): NetMgmt consists of systems used to support global network Fault, Configuration, Accounting, Performance, and Security Management.

### **9.3 Network Concepts & Requirements**

The Contractor shall conduct requirements analysis to ensure that system level requirements are properly allocated to the network and incorporated into BMDS Communications Network Implementation Specification (BCNIS). The Contractor shall present an out brief of the deliverable BCNIS product IAW DI-SESS-81309A (CDRL-A084). The Contractor shall conduct trade studies to assess alternative design approaches and to confirm technical feasibility of recommended alternative. The Contractor shall develop System Concepts for the Network for Spiral 8.2 and coordinate and develop these concepts with the Architecture Working Group (AWG) and C2BMC. The Contractor shall include Network requirements in the Element Requirements Review for Spiral 8.2, coordinate Network Requirements, and maintain traceability of requirements in a database with Government access. This database will be established at the onset of this contract and shall be program specific.

### **9.4 Information Exchange Requirements (IER)**

The Contractor shall develop Information Exchange Requirements (IER) for the C2BMC element and the interfaces with Elements, COCOMs, and the SIPRNET. The Contractor shall determine information exchange rates for all IERs. The Contractor shall deliver IERs with associated exchange rates in DI-IPSC-81434 (CDRL-A085).

### **9.5 Network Model**

The Contractor shall conduct high fidelity Network Modeling and Capacity Utilization Modeling to assess network performance and guide the network design effort.

## **9.6 Network Design**

The Contractor shall design the Network for Spiral 8.2 to meet the requirements agreed upon in the Spiral Content Agreement (SCA) and the requirements as specified in C2BMC Element and Spiral Specifications. The Contractor shall develop and maintain a Network Development Laboratory (NDL) to verify and test Spiral 8.2 design. The Contractor shall participate in Spiral 8.2 system level Design Reviews and conduct associated Network level Design Reviews.

The network design shall support an Enterprise Architecture that includes either a semi-centralized management core or live Continuity of Operations (COOP) to operate across the globe supporting operations in more than one hemisphere.

### **9.6.1 Network Security Design**

The Contractor shall ensure that IA engineers participate in network design activities to ensure that proposed security tools and concepts are instantiated properly in the network design and to identify and mitigate or correct security flaws in the working network design. The security design shall be in accordance with DoDI 8500 series.

### **9.6.2 Network Trades**

The Contractor shall conduct trade studies in collaboration with Government, Federally Funded Research & Development Center (FFRDC) and Advisory & Assistant Services (A&AS) in the areas of CNE function and performance, vendor selection, architectural alternatives, IP routing to assess alternative design approaches and to confirm technical feasibility of recommended alternatives. The results of these trade studies support both concept formulation and requirements analysis.

## **9.7 Network Integration & Test**

The Contractor shall conduct Network Integration and Testing (I&T) of the BCN products to verify that their performance meets the relevant requirements, specifications, and standards. The Contractor shall meet the industry best practices if no specific requirements, standards, or specifications are available. The Contractor shall develop network integration and test plans and procedures for use in verification of the BCN product capabilities. The Contractor shall provide network integration and test procedures to C2BMC for review and approval. The Contractor shall support the Product Integration Laboratories (PIL) in conducting integration and testing. The Contractor shall complete integration and testing for Network Spirals at Missile Defense Integration and Operations Center (MDIOC) to support deployment of the PSN/RTB and resolve SMRs that arise during PSN/RTB testing and utilization. The Contractor shall support deployment to the PSN/RTB, providing Net Hardware/Software installation support and resolution of Network related SMRs that arise during testing and utilization of PSN/RTB. The Contractor shall provide support for conducting simulations of “what if” deployments, and network expansions as required by the Government. The Contractor shall provide a report on network capacity utilization, based on network modeling and simulation, real world ops, PSN and test events IAW DI-MISC-80711. The Contractor shall manage a BNOSC Analysis and Test Suite (BATS).

### **9.8 Network System Integration and Test Environment (NSITE)**

The Contractor shall incorporate only Government approved taps, as directed in writing by the C2BMC Program Office, into each spiral design, to enable connection of NSITE equipment. Design changes will include incorporating taps into each spiral and taps will be documented in network engineering drawings.

### **9.9 Trouble Ticketing/ Work flow System**

The Contractor shall provide a Trouble ticketing system that includes a SIPRNET Web site, where Trouble tickets can be opened, inspected, updated, and closed. The system shall include automated trouble ticket generation capabilities (e.g. receive inputs on outages from Network Management and IA/CND equipment). The system shall include aspects of the Information Technology Infrastructure Library methodology e.g. Configuration Management Database (CMDB) incident identification, problem elevation, root cause analysis and configuration management. The system shall follow or be compatible with the MDA standard system IAW Chief Information Officer (CIO) direction. The system shall integrate with the Network Operations (NetOps) Visibility and Analysis System (NOVAS) and/or a User Defined Operational Picture.

The Contractor shall support use of and modify as needed an automated common workflow process system, following the Information Technology Infrastructure Library (ITIL) model, as identified by trade study, industry best practices, common MDA approved products list or open research, e.g. Gartner Report or equivalent. Product selection is described in greater detail in the Development Task Order.

### **9.10 Data Collection and Analysis**

Network IPT shall collect referent data during Flight tests, Ground Tests, and Target of opportunities and shall perform data reduction and analysis. The purpose of this data collection is to determine areas of improvement within the network design, confirmation of Network requirements, and failure analysis.

## **10.0 CONCURRENT TEST, TRAINING AND OPERATION (CTTO)**

The Contractor shall assist the Government to plan, design, develop, deploy, integrate, operate, sustain, and remove the C2BMC, BMDS, and Integrated Air and Missile Defense (IAMD) test and training systems that enhance the ability of the BMDS to conduct testing, training, and exercises with friend and allies without negatively impacting operations. The Contractor shall meet safety requirements in BMDS System Specification for CTTO.

## **11.0 SUPPORT REAL WORLD OR CONTINGENCY OPERATIONS**

The Contractor shall execute special emphasis tasks that include implementation of technical study results or recommendations; analyses, assessments, and reports; issue resolutions for C2BMC; procurement of material; software updates/engineering releases; facility changes; technical support to Government M & S (independent assessments); and ground/flight events and exercises. The Contractor shall maintain flexibility to call upon various degrees and types of support. Support could entail supporting mission priorities, real world deployments, and

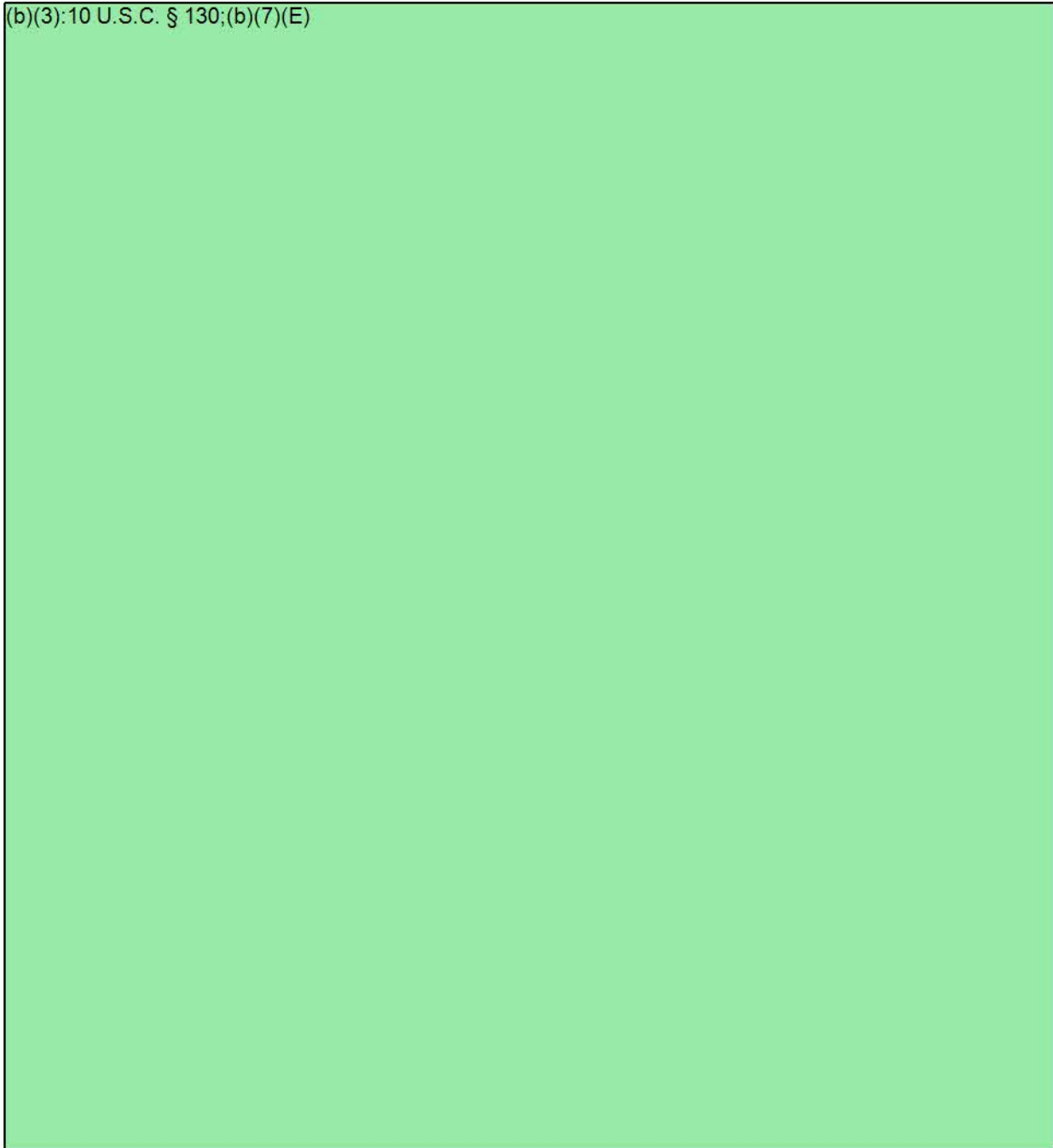


contingency events both CONUS and OCONUS. Results shall be delivered to the Government IAW instructions in the Task Instruction(s).

### **12.0 Places of Performance**

The Contractor shall perform the efforts under this Contract at the following locations, where classified information may need to be accessed and in some cases stored, as authorized and in accordance with the requirements of Attachment 2, DD 254 - Security Classification Document, associated with this Contract. The Contractor shall have access to these locations in fulfillment of the Task Order terms and conditions.

(b)(3):10 U.S.C. § 130;(b)(7)(E)

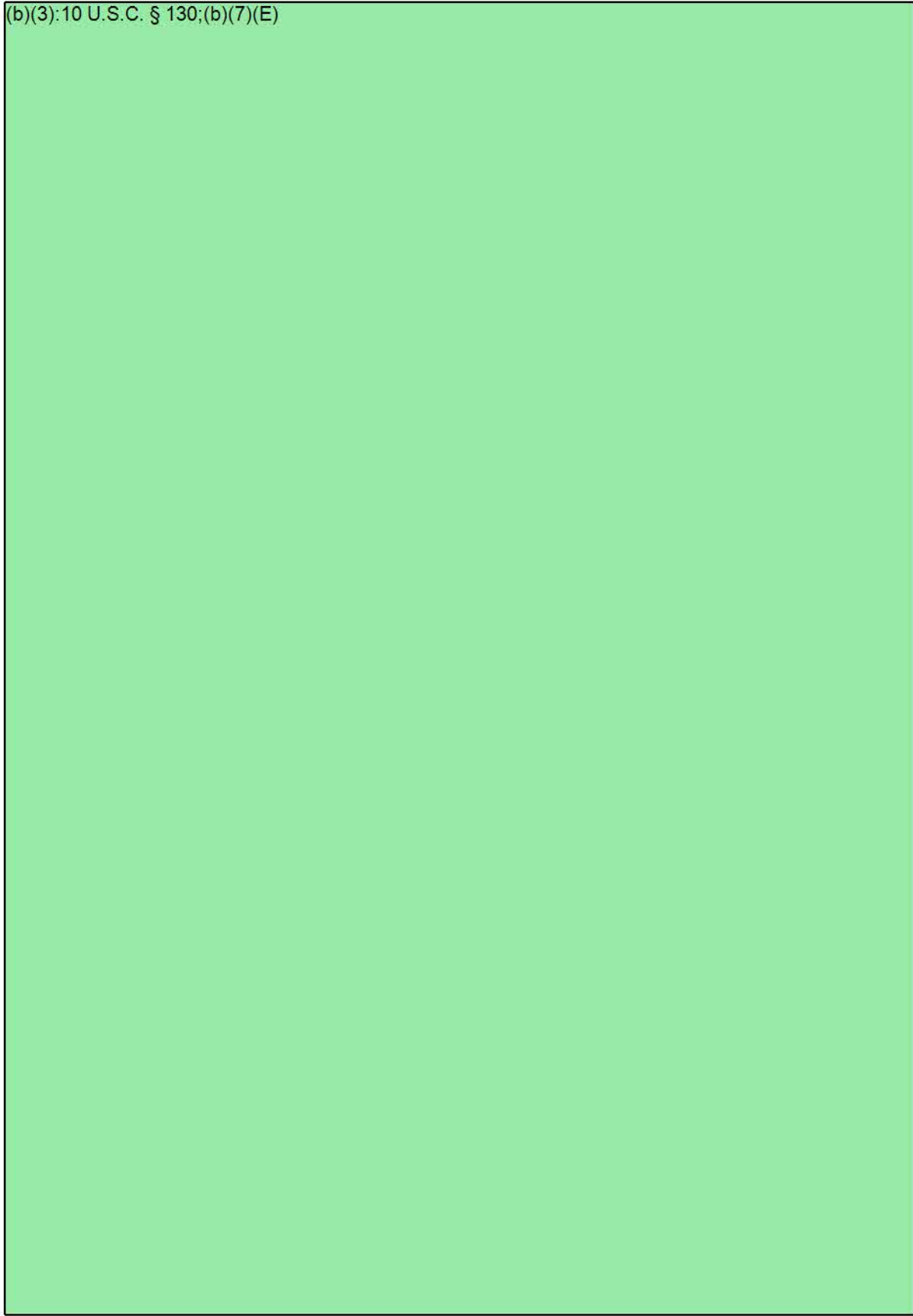


(b)(3):10 U.S.C. § 130;(b)(7)(E)

(b)(3):10 U.S.C. § 130;(b)(7)(E)



(b)(3);10 U.S.C. § 130;(b)(7)(E)





### **13.0 Acronym List**

A&AS	Assistance and Advisory Services
A&SE	Architecture & System Engineering
ABIR	Airborne Infrared
ADSI	Air Defense System Integrator
ADMIN	Administrative
AMDWS	Air & Missile Defense Workstation
AN/TPY-2	Army Navy / Transportable Radar Surveillance - Model 2
AOC	Air Operations Center
AOR	Area of Responsibility
ARBTS	Automated Release Baseline Tracking
ASEMP	Architecture and Systems Engineering Management Plan
AT	Anti-Tamper
ATO	Authority to Operate
ATP	Acceptance Test Plan
AWG	Architecture Working Group
BATS	BNOSC Analysis and Test Suite
BCM	BMDS C2BMC Model
BCN	BMDS Communications Network
BCNIS	BMDS Communications Network Implementation Specification
BMD	Ballistic Missile Defense
BMDS	Ballistic Missile Defense System
BMDSS	Ballistic Missile Defense System Specification
BNOSC	BMDS Network Operations Support Center
BNOSC-C	BMDS Network Operations Support Center - C2BMC
BOM	Bill of Material
BTIR	BMDS Test Incident Report
C2BMC	Command Control, Battle Management and Communications
C&A	Certification and Accreditation
CAC	Common Access Card
CAGE	Commercial and Government Entity
CARD	Cost Analysis Requirements Description

CBS	C2BMC Build Specifications
CCB	Configuration Control Board
CWBS	Contract Work Breakdown Structure
CWG	Cost Working Group
CDP	Certification Data Package
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDS	Cross-domain-solution
CEC	Critical Engagement Condition
CESB	C2BMC Event Scheduling Board
CFSR	Contract Funds Status Report
CIO	Chief Information Officer
CLIN	Contract Line Item Number
CM	Configuration Management
CMDB	Configuration Management Database
CMP	Configuration Management Plan
CND	Computer Network Defense
COCOM	Combatant Commanders
COMSEC	Communication Security
CONOPS	Continuity of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-off-the-Shelf
CP	Consolidation Plan
CPR	Contract Performance Report
CPS	C2BMC Performance Specifications
CPT	Cross-Product Team
CR	Change Request
CRSP	Computer Resource Support Plan
CPS	C2BMC Performance Specifications
CSDR	Cost and Software Data Reporting
CSS	C2BMC Spiral Specifications
CT&E	Certification, Test and Evaluation
CTOWG	C2BMC Test Objectives Working Group
CTTO	Concurrent Test, Training and Operations
CUBE	C2BMC Control Center
CWBS	Contract Work Breakdown Structure
CWG	Cost Working Group
DAA	Designated Accrediting Authority/Designated Accreditation Authority
DAL	Data Accession List
DDD	Display Description Document
DESim	Discrete Event Simulation
DEV	Development
DI	Data Item

DIA	Defense Intelligence Agency
DIACAP	Department of Defense (DoD) Information Assurance Certification and Accreditation Process
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISR	Department of Defense (DoD) Information Technology Standards Registry
DISN	Defense Information Systems Network
DISR	Department of Defense Information Technology Standards Registry
DM	Data Management
DPAS	Defense Priorities and Allocations System
DTS	Distributed Training System
DMS	Diminishing Manufacturing Sources
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOORS	Dynamic Object-Oriented Requirements System
DR	Disaster Response
DRSN	Defense Red Switch Network
DSA	Digital Simulation Architecture
DSB	Data Scoring Board
DSS	Defense Security Services
DTTP	Doctrine, Tactics, Techniques and Procedures
EDS	Electrostatic Discharge
EIA	Engineering Industries Association
EME	Empirical Measurement Events
ENVR	Environmental Reporting
ESOH	Environment, Safety, and Occupational Health
ESWG	Element Safety Working Group
EVM	Earned Value Management
EVMS	Earned Value Management System
EWS	Enterprise Work Station
FADD	Functional Area Design Description
FAR	Federal Acquisition Regulations
FFRDC	Federally Funded Research & Development Center
FMECA	Failure Modes Effects and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and Corrective Action System
FRB	Failure Review Board
FTA	Fault Tree Analysis
GEM	Global Engagement Management
GENSER	General Service
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFS	Government Furnished Services
GIDEP	Government Industry Data Exchange Program
GOTS	Government Off-The-Shelf
HAIPE	High Assurance Internet Protocol Equipment

HDBK	Handbook
HEMP	High-Altitude Electromagnetic Pulse
HFE	Human Factors Engineering
HN	Host Nation
HTS	Hazard Tracking System
HW/SW	Hardware/Software
HW	Hardware
HWIL	Hardware-in-the-Loop
I2RSS	Imaging Infrared Simulation System
I&S	Interoperability & Supportability
I&T	Integration & Testing
IA/CND	Information Assurance/Computer Network Defense
IA	Information Assurance
IAEB	Information Assurance Engineering Board
IAM	Information Assurance Manager
IAMD	Integrated Air and Missile Defense
IAO	Information Assurance Officer
IATF	Information Assurance Technical Framework
IATO	Interim Authority to Operate
IATT	Interim Authority to Test
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IBCS	Integrated Air and Missile Defense Battle Command System
IBR	Integrated Baseline Review
ICCB	Internal Configuration Control Board
ICD	Interface Control Document
ICS	Interface Control Specification
IDD	Interface Design Document
IDE	Integrated Digital Environment
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IER	Information Exchange Requirements
IFS	Interface Specification
IG	Inspector General
ILS	Integrated Logistics Support
ILSP	Integrated Logistics Support Plan
IMAP	Integrated Master Assessment Plan
IMP	Integrated Master Plan
IMS	Integrated Master Schedule
IMTP	Integrated Master Test Plan
IP	Internet Protocol
IPPD	Integrated Process and Product Development
IPT	Integrated Product Team



IRP	Incident Response Procedures
ISO	International Organization for Standardization
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISSPP	Integrated System Safety Program Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IUID	Item Unique Identification
IV&V	Independent Verification and Validation
JAT	Joint Analysis Team
JFCC-IMD	Joint Forces Component Command for Integrated Missile Defense
JIT	Joint Interface Test
JRMET	Joint Reliability & Maintainability Evaluation Team
JTF-GNO	Joint Task Force-Global Network Operations
KG	Key Generator
KTP	Key Test Point
LHCT	Long-Haul Communication Transport
M&S	Modeling & Simulation
MAC	Mission Assurance Capability
MAIP	Mission Assurance Implementation Plan
MAP	Missile Defense Agency Assurance Provision
MCP	Mutual Commitment Package
MCSB	Mission Control Station Backup
MDA	Missile Defense Agency
MDA/BC	C2BMC Program Office
MDACNet	Missile Defense Agency Classified Network
MDAUNet	Missile Defense Agency Unclassified Network
MDIOC	Missile Defense Integration and Operations Center
MiDAESS	Missile Defense Agency Engineering and Support Services
MIDB	Modernized Integrated Database
MIPS	Maritime IAMD Planning System
MOA	Memorandum of Agreement
MOSA	Modular Open Systems Approach
MP	Message Processing
MRB	Material Review Board
MTBF	Mean Time Between Failures
MTTR	Mean Time to Restore
OEM	Original Equipment Manufacturer
OMC	Operations Migration Capability
OOB	Out of Band
OPR	Office of Primary Responsibility
OWG	Obsolescence Working Group
NDL	Network Development Laboratory
NEPA	National Environmental Policy Act
NetCore	Core Network
NetMgmt	Network Management

NetOps	Network Operations
NetSec	Network Security
NDI	Non-Development Item
NDL	Network Development Laboratory
NIPRNET	Non-Classified Internet Protocol Router Network
NIRP	Network IPT Review Panel
NIST	National Institute of Science and Technology
NMS	Network Management System
NOVAS	NetOps Visibility and Analysis System
NR-KPP	Net Ready-Key Performance Parameter
NSA	National Security Agency
NSITE	Networked Solutions Integration Test Engineering
O&S	Operation & Sustainment
OEM	Original Equipment Manufacturer
OOB	Out of Band
OPIR	Overhead Persistent Radar
OPSCON	C2BMC Operational Concept
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OSHA	Occupational Safety & Health Administration
OTA	Other Transaction Agreement
OWG	Obsolescence Working Group
OWS	Operator Workstation
P2P	Peer-to-Peer
PCB	Program Change Board
PCO	Procurement Contracting Officer
PDSS	Post-Deployment Software Support
PERB	Program Engineering Review Board
PESHE	Programmatic Environmental, Safety & Health Evaluation
PHST	Package, Handling, Storage and Transportation
PIL	Product Integration Laboratory
PIT	Product Integration Team
PKI	Public Key Infrastructure
PMAP	Parts, Materials, & Processes Mission Assurance Plan
PMP	Parts, Materials, & Processes
POA&M	Plan of Actions, and Milestones
PPP	Program Protection Plan
PR	Problem Report
PRD	Program Report Database
PSN	Parallel Staging Network
PSN/RTB	Parallel Staging Network/Regional Test Bed
PSSP	Product Specific Support Plan
PTSS	Precision Tracking Space System
QA	Quality Assurance
QA/MAWG	Quality Assurance/Mission Assurance Working Group
QAP	Quality Assurance Provisions

QAPP	Quality Assurance Program Plan
QS	Quality, Safety, and Mission Assurance
QSMA	Quality, Safety, and Mission Assurance
RAM	Requirements Applicability Matrix
RAMT	Reliability, Availability, Maintainability & Testability
RCI	Reliability Critical Items
RDTE	Research, Development, Test & Evaluation
RF	Radio Frequency
RMWG	Risk Management Working Group
ROM	Rough Order of Magnitude
RTB	Regional Test Bed
S6.4C2	Spiral 6.4C2
S8.2	Spiral 8.2
SAR	Safety Assessment Report
SARAD	System Architecture and Requirements Allocation Description
SAV	Staff Assistance Visit
SBIRS	Space Based Infrared Sensor
SCA	Spiral Content Agreement
SCAR	Spiral Capability Assessment Report
SCM	Software Configuration Management
SCR	Software Change Report
SCVP	Spiral Capability Verification Plan
SDE	Software Development Environment
SDF	Software Development Folder
SDP	Software Development Plan
SDR	Software Data Reporting
SE	Support Equipment
SE/TMDE	Support Equipment/Test Measurement and Diagnostic Equipment
SEMP	System Engineering Management Plan
SETA	Systems Engineering and Technical Assistance
SICD	System Interface Control Document
SIE	Special Inspection Equipment
SIP	Software Installation Plan
SIPRNet	Secret Internet Protocol Router Network
SME	Subject Matter Expert
SMP	Software Maintenance Plan
SMR	Software Modification Request
SOW	Statement of Work
SP	Synchronization Plan
SPEAR	Synchronization of Program Execution Activity Roundtable
SPFR	System Post-Flight Reconstruction
SPP	Standard Practice and Procedure
SQA	Software Quality Assurance
SRR	Shipping Readiness Review
SRTM	Security Requirements Traceability Matrix
SSHA	Subsystem Hazard Analysis

SSPP	System Safety Program Plan
SSQ	Site Survey Questionnaire
SSR	Summary Subcontracting Report
SSS	System/Subsystem Specifications
SSWG	System Safety Working Group
STE	Special Test Equipment
STIGS	Security Technical Implementation Guides
SUT	System Under Test
SW	Software
SwSWG	Software System Safety Working Group
TBD	To Be Determined
TCWG	Test Configuration Working Group
TE	Technical Expert
TESA	Technical Expert Status Accreditation
THAAD	Terminal High Altitude Area Defense
TIM	Technical Interchange Meeting
TMDE	Test Measurement and Diagnostic Equipment
TOM	Test Objective Memorandum
TP	Transition Plan
TPM	Technical Performance Measurement
TPS	Test Program Sets
TRR	Test Readiness Review
TS/SCI	Top Secret/Sensitive Compartmented Information
TTP	Tactics, Training, and Procedures
USAF	United States Air Force
V&V	Verification and Validation
VLAN	Virtual Local Area Network
VMS	Vulnerability Management System
WAS-UP	Weekly Analysis Status Update
WBS	Work Breakdown Structure
WF	Warfighter
WIP	Warfighter Involvement Process
WPI	Work Product Inspection