DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

- ☒ a. PRIME CONTRACT NUMBER: HQ0147-12-D-0003
- ☐ b. SUBCONTRACT NUMBER
- ☐ c. SOLICITATION OR OTHER NUMBER — Due Date *(YYYYMMDD)*:

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

- ☐ a. ORIGINAL *(Complete date in all cases)* — Date *(YYYYMMDD)*: 2011/12/21
- ☒ b. REVISED *(Supersedes all previous specs)* — Revision No.: 4 — Date *(YYYYMMDD)*: 2017/04/04
- ☐ c. FINAL *(Complete Item 5 in all cases)* — Date *(YYYYMMDD)*:

4. IS THIS A FOLLOW-ON CONTRACT? ☒ YES ☐ NO. If Yes complete the following

Classified material received or generated under HQ0006-02-9-0002 *(Preceding Contract Number)* is transferred to this follow-on contract

5. IS THIS A FINAL DD FORM 254? ☐ YES ☒ NO. If Yes complete the following

In response to the Contractor's request dated _____, retention of the identified classified material is authorized for the period of _____.

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Lockheed Martin Corporation 9970 Federal Drive Colorado Springs, CO 80921	60854	Defense Security Service (IOFWC)

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICES *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
See Block 13, Reference Item 8.a.		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Missile Defense Agency, Command and Control, Battle Management and Communications (C2BMC)

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☒	☐	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☒
b. RESTRICTED DATA	☒	☐	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☒
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☒	☐	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☒	☐
d. FORMERLY RESTRICTED DATA:	☒	☐	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☒	☐
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	☐	☒
(1) Sensitive Compartmented Information (SCI)	☒	☐	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☒	☐
(2) Non-SCI	☒	☐	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☒	☐
f. SPECIAL ACCESS INFORMATION	☒	☐	h. REQUIRE A COMSEC ACCOUNT	☒	☐
g. NATO INFORMATION	☒	☐	i. HAVE A TEMPEST REQUIREMENT	☐	☒
h. FOREIGN GOVERNMENT INFORMATION	☒	☐	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☒	☐
i. LIMITED DISSEMINATION INFORMATION	☐	☒	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☒	☐
j. FOR OFFICIAL USE ONLY INFORMATION	☒	☐	l. OTHER *(Specify)* – Restrict Access to Contractor's Unclassified Automated Information System (AIS). – Requires CNet/SIPR/JWICS	☒	☐
k. OTHER *Specify)* NC2-ESI	☒	☐			

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release

☐ Direct ☒ Through *(Specify):*

Missile Defense Agency/BC
5224 Martin Road
Redstone Arsenal, AL 35898

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the Contractor is authorized and encouraged to provide recommended changes: to challenge the guidance or classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

The Contractor is required to flow-down all applicable requirements of the DD Form 254 to its Subcontractor(s).

Direct all questions pertaining to the DD Form 254 to the MDA Industrial Security office by phone at 256-313-9429, by email at MDAIndustrialSecurity@mda.mil, or by mail to MDA, ATTN: Industrial Security Office (EIR), Building 5222 Martin Road, Redstone Arsenal, AL 35898.

Contracting Officer's Representative (COR) DD Form 254 Concurrence:

(b)(6)

See Continuation Pages (3-13)

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. *(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)* ☒ Yes ☐ No

See Reference Items; 10.e.(1), 10.f, 10.j, 11.j, 11.l. and 14.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. *(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.* ☐ Yes ☒ No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
(b)(6)	Contracting Officers Security Representative	(b)(6)

d. ADDRESS *(Include ZIP Code)*
Missile Defense Agency
5222 Martin Road
Redstone Arsenal, AL 35898

e. SIGNATURE
(b)(6)

17. REQUIRED DISTRIBUTION

- ☒ a. CONTRACTOR
- ☐ b. SUBCONTRACTOR
- ☒ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- ☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- ☒ e. ADMINISTRATIVE CONTRACTING OFFICER
- ☒ f. OTHERS AS NECESSARY MDA Industrial Security

SECURITY GUIDANCE (BLOCK 13) CONTINUATION PAGES:

Special Instructions:

Reporting Requirements:

The Contractor shall provide the following to the MDA Industrial Security Office (contact information listed in block 13 of page two of the DD Form 254):

- Courtesy copy the MDA Industrial Security Office on any security incident report (initial and final) involving the loss, compromise, or suspected compromise of classified information sent to the Defense Security Service. The Contractor shall provide a copy to the MDA within the same reporting timeframe as is required by the Defense Security Service (72 hours for Secret/Confidential and 24 hours for Top Secret)
- Courtesy copy the MDA Industrial Security Office on any report involving a cyber-intrusion of MDA program information sent to the Federal Bureau of Investigation and the Defense Security Service per NISPOM Chapter 1, Section 301 and Industrial Security Letter 2013-05.
- Provide a copy of any Defense Security Service letter that indicates a less than satisfactory security rating and/or that negatively impacts the Facility Clearance Level (FCL) of the company within 48-hours of receipt.
- Provide electronic copies of Subcontractor DD Form 254s issued by the Prime and the Subcontractor. The Prime Contractor shall act as the focal point for collecting their Subcontractor's DD Form 254s and the Prime is responsible for forwarding these DD Form 254s to the MDA Industrial Security Office.

In accordance with NISPOM Chapter 1, Section 300, the Contractor and its subcontractors shall notify the Contracting Officer, the Contracting Officer's Representative, and MDA Industrial Security in writing within 24 hours of becoming aware of adverse information regarding an employee, who works within a Government/MDA facility, which could affect their access to classified information. Reportable information is described in DoD Regulation 5200.2-R, paragraph C2.2.1. and Appendix 8.

Subcontractor Classified Access Approvals:

The Prime Contractor and Subcontractor are authorized to flow access to and/or dissemination of classified information to the TOP SECRET level to their Subcontractor. Dissemination is only authorized and applicable for information safeguarded at the Contractor's facility. This authorization includes access to Non-Sensitive Compartmented Information (SCI) (NISPOM Chapter 9, Section 304), Communications Security (COMSEC) (NISPOM Chapter 9, Section 407), Critical Nuclear Weapon Design Information (CNWDI) (NISPOM Chapter 9, Section 204), and North Atlantic Treaty Organization (NATO) (NISPOM Chapter 10, Section 708) information. The Contractor shall provide the appropriate accesses to its Subcontractors as required per NISPOM 5-502. The Prime Contractor and Subcontractor must verify Facility Clearance, Safeguarding Capability and Access Authorizations prior to the dissemination of classified information. The following require specific authority: SCI - not authorized to flow without prior approval from MDA/Special Security and Special Access Program (SAP) - not authorized to flow without prior approval from MDA/Special Programs.

Reference Item 8.a. (continued) Government Locations:
Classified performance will occur at various MDA and/or government locations as directed by the contract via the Performance Work Statement, Statement of Work, or Statement of Objectives or other agreement. The Contractor shall abide by the host government security requirements per NISPOM Chapter 1, Section 200 and Chapter 6, Section 105c. The cognizant security office at the performance location is MDA or the host installation.

Reference Item 8.a. (continued) Performance Locations include the following Contractor Facilities:

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE
Lockheed Martin Corporation 9970 Federal Drive Colorado Springs, CO 80921	60854	Defense Security Service (IOFWC)

Per NISPOM Chapter 5 Section 504, the Contractor can disclose classified information between cleared facilities within the Multiple Facility Organization (MFO). MDA does not limit which cleared locations are considered performance locations within the MFO. It is the Contractor's responsibility to comply with Defense Security Service policy and procedures for establishing a classified performance location within the MFO structure. This guidance does not apply to government locations or other Contractor company locations at which the prime Contractor will be conducting classified performance.

Reference Item 10.a. and 11.h: The Contractor shall comply with the requirements of NISPOM Chapter 9, Section 4 and National Security Agency/Central Security Service Policy Manual Number 3-16, Control of Communications Security (COMSEC) Material, for access to and safeguarding of COMSEC information.

Reference Item 10.b & d: Contractors shall adhere to the requirements of DoDI 5210.02, "Access to and Dissemination of Restricted Data (RD) and Formerly Restricted Data (FRD)," 3 June 2011, for access and training requirements. **Flow this requirement to subcontractors when applicable.**

1. Contractors shall possess a valid DoD security clearance at a level commensurate with the information concerned and shall have a need-to-know for access. DoD contractors require a final Secret security clearance for access to Secret RD information. Contractors shall have a final Top Secret security clearance for access to Top Secret RD information. NISPOM section 2-211a. applies.

2. The Prime contractor and its subcontractors shall be required to complete training for access to RD/FRD material and for derivative classification of RD/FRD information. This training is provided by the Department of Energy (DOE) and can be accessed at the DOE website (http://energy.gov/hss/services/classification/classification-training-institute/training-other-agency-personnel).

a. For individuals with access to RD/FRD information, personnel shall complete the "Classification of Nuclear Weapons-Related Information (Restricted Data and Formerly Restricted Data)" course. The contractor company shall maintain a record of the training for each individual with access to RD/FRD. These records shall be made readily available during security inspections or for other government purposes. Records shall be maintained for two years after an individual no longer requires access to RD/FRD information.

b. For individuals who will conduct derivative classification, personnel shall complete the "Restricted Data Classifiers Course." The contractor company shall maintain a record of the training for each individual designated as a RD Classifier. These records shall be made readily available during security inspections or for other government purposes. Records shall be maintained for two years after an individual is no longer designated as a RD Classifier.

Reference Item 10.c: NISPOM Chapter 9, Section 2 requirements apply. Access to Critical Nuclear Weapons Design Information requires a final clearance.

Reference Item 10.e.(1): This contract requires access to Sensitive Compartmented Information (SCI) material. The Contractor is not required to have an accredited SCI Facility but requires access to SCI at other locations. Additionally, the Facility Security Officer will ensure that when a Contractor with access to SCI is due for a Periodic Reinvestigation, the Periodic Reinvestigation request is conducted to meet SCI standards. Written U.S. Government approval by MDA/Special Security is required prior to giving SCI access to a Subcontractor. Additional requirements are included in the attached SCI Supplement.

Reference Item 10.e.(2): NISPOM Chapter 9, Section 3 requirements apply.

Reference Item 10.f: Requirements are included in the attached SAP Supplement.

Reference Item 10.g: NISPOM Chapter 10, Section 7 requirements apply.

Reference Item 10.h: NISPOM Chapter 10, Section 3 requirements apply.

Reference Item 10.j: See For Official Use Only/Controlled Unclassified Information (FOUO/CUI) Supplement below. **The Contractor is required to provide the supplement to all uncleared Subcontractors requiring access to FOUO/CUI information.**

Reference Item 10.k:

1. This contract requires access to Nuclear Command and Control Extremely Sensitive Information (NC2-ESI). NC2-ESI material remains under US Government control at all times. Access to NC2-ESI by Contractor personnel will be limited to US Government facilities.

2. In order to be considered for access to NC2-ESI, applicant must be a United States citizen. No waivers will be considered. In addition, applicant must have a Top Secret clearance based on a favorable Single Scope Background Investigation (SSBI) completed within the past five years. No waivers will be considered.

3. Contractor will nominate personnel according to CJCSI 3231.01B. Contractor will nominate only technically qualified personnel who meet citizenship and clearance requirements stated above.

4. Nominations will contain full identifying data on the nominee, statement that he/she meets the above citizenship requirements, description of the applicant's duties under the contract, which will require access to NC2-ESI, applicant's current clearance and the basis for the clearance.

5. If the applicant meets the clearance and investigation criteria, nomination must be received by USSTRATCOM/J050, 30 days prior to anticipate date NC2-ESI access is required.

6. NC2-ESI access will require briefing and debriefing to be accomplished by local NC2 Program Managers or Security Managers. A copy of the briefing must be forwarded to USSTRATCOM/J050.

7. Contractor will advise local NC2 Program Managers of any adverse information or change in status of an employee who has been granted access to NC2-ESI, i.e., marriage, divorce or remarriage.

Reference Item 11.c: The contractor shall be required to track classified information sent via non-electronic and obtain a receipt from the recipient (reference NISPOM Chapter 5, Section 401b.). The tracking method used by the contractor shall ensure daily tracing (excluding weekends and holidays), and any loss or compromise of the classified information shall be reported in the timeframes established in the "Reporting Requirements" section of this DD Form 254. The Contractor has a responsibility to understand and use all applicable Security Classification Guidance (SCG) provided by the government (reference NISPOM 4-102). The MDA has provided a list below of necessary SCGs required to conduct derivative classification. The Contractor shall request the required SCGs from the Contracting Officer's Representative (COR). The MDA has the obligation to review existing guidance periodically during the performance stages of the contract and to issue a revised DD Form 254 when a change to the SCGs occurs or when additional SCGs are needed (reference NISPOM Chapter 4, Section 103b.). The Contractor shall flow-down required SCGs on its Subcontractor DD Form 254s and shall provide copies of the SCGs to its Subcontractor. The following security classification guidance applies:

1. Ballistic Missile Defense System (BMDS) Security Classification Guide (SCG), dated 19 October 2010 to include Admin Changes dated 11 July 2011.
2. Ground-Based Midcourse Defense (GMD) Security Classification Guide (SCG), dated 07 August 2006, to include Admin Changes dated 11 July 2011.
3. Space Based Infrared System (SBIRS) Security Classification Guide (SCG), dated 15 June 2007.
4. Patriot Air and Missile Defense System Security Classification Guide (SCG), dated 07 February 2012.
5. Airborne Laser (ABL) Security Classification Guide (SCG), dated 27 May 2003, to include Admin Changes dated 22 August 2011.
6. Terminal High Altitude Area Defense (THAAD) Security Classification Guide (SCG), dated 29 November 2001, to include Admin Changes dated 29 December 2014.

7. Ballistic Missile Defense (BMD) Radars Security Classification Guide (SCG), dated 22 July 2013.
8. Air Force Technical Applications Center (AFTAC) Radar Sensor Platform Security Classification Guide (SCG), dated 03 Mar 2008, to include Admin Changes dated 01 July 2011.
9. Aegis Ballistic Missile Defense (ABMD) Security Classification Guide (SCG), dated 08 November 2005, to include Admin Changes dated 11 July 2011.
10. OPNAVINST S5513.3F, Standard Missile 2/3/4/6, Security Classification Guide (SCG) dated 01 October 2012.
11. Anti-Tamper (AT) Security Classification Guide (SCG), dated 17 March 2010, to include Change Letter 2, dated 19 May 2014
12. DoDI S-5230.28, Low Observable (LO) and Counter Low Observable (CLO) Programs (U), 28 May 2005.
13. CG-W-5, Joint DOE/DOD Nuclear Weapon Classification Policy Guide, dated May 24, 2004 and currently incorporated changes thereto. Prior to receipt of this document, contractors must obtain appointment of individuals to serve as official RD Classifiers IAW the NISPOM and DOE guidelines. This appointment is required for derivative classification authority and generation of RD/FRD material for all related facilities and systems.
14. Other Security Classification Guides will be provided as required.

Reference Item 11.d: The Contractor is required to provide adequate storage and transportation for classified hardware to the level of SECRET. If the classified hardware is of such a size or quantity that it cannot be safeguarded in a regular-sized GSA-approved storage container, a Closed Area, Vault, or additional security containers may be required. Per the NISPOM, the Defense Security Service has responsibility for the authorization and approval of all Closed Areas and/or Vaults within the Contractor's facility.

Reference Item 11.f:

1. The Contractor shall require access to classified information overseas at areas designated in the Statement of Work, Performance Work Statement, or Statement of Objectives.

2. All Contractor personnel working at the designated location(s) and accessing classified information shall obtain an Area of Responsibility-specific travel briefing and Antiterrorism Level I Awareness training prior to departing on travel. Required training shall be received within 90 days prior to travel.

3. The Contractor shall submit foreign visit requests as dictated by the NISPOM, Chapter 10, Section 5. A Contractor shall submit the visit request through the Defense Security Service-designated security official.

4. The Contractor is not authorized per the NISPOM to establish a contractor facility outside of the U.S., its possessions, or its territories. Storage, custody, and control of classified information required by a U.S. Contractor employee abroad is the responsibility of the U.S. Government. Storage of classified information shall be at a U.S. military facility, a U.S. Embassy or Consulate, or another location occupied by a U.S. Government organization.

Reference Item 11.g: The Contractor is authorized to use the services of the Defense Technical Information Center (DTIC) or other secondary distribution center. As required, the Contractor will prepare and submit the DD Form 1540, "Registration for Scientific and Technical Information Services" and DD Form 2345, "Militarily Critical Technical Data Agreement" to the contracting office for approval. Subcontractors are required to submit requests through the Prime Contractor.

Reference Item 11.j: The Contractor is required to apply Operations Security (OPSEC) to enhance protection of classified and unclassified critical information pursuant to DoD Directive 5205.02, "DoD OPSEC Program; DoD 5205.02-M, "OPSEC Program Manual;" National Security Decision Directive Number 298, "National Operations Security Program;" MDA Instruction 5205.02, "OPSEC Program;" and supplementary instructions. Service OPSEC guidance may also apply if the contracted activity is performed in a Service-level operational environment. If a conflict is identified between Service and higher-level guidance, contact the MDA OPSEC Staff for clarification.

Reference Item 11.l:

Contractor's Unclassified Automated Information System (AIS):

1. The Contractor shall safeguard and protect Controlled Unclassified Information provided by or generated for the Government (other than public information) that transits or resides on any non-Government information technology system IAW the procedures in DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, Enclosure 3. Information shall be protected from unauthorized access, disclosure, incident or compromise by extending the safeguarding requirements and procedures in DFARS clause 252.204-7012, Safeguarding of Covered Defense Information and Cyber Incident Reporting. The NIST 800-171 security controls specified in 252.204-7012 was extended to include Controlled Unclassified Information (CUI) information which resides on, or transits through the contractor's (prime and all sub-contractors) unclassified information technology systems.

2. The contractor shall ensure that all persons accessing CUI, which includes FOUO, meet the qualifications for an Automated Data Processing/Information Technology (ADP/IT)-III Position requirement).

3. The "For Official Use Only/Controlled Unclassified Information Supplement" provides additional guidance for the handling, marking, transmission, reproduction, safeguarding, and disposition of FOUO/CUI.

4. MDA-reserves the right to conduct compliance inspections of Contractor unclassified information systems and other repositories for the protection of FOUO/CUI.

Reference Item 12: The Prime Contractor shall forward all requests for public release authorization through the Contracting Officer's Representative to the listed MDA program office. Per NISPOM section 5-511, the Contractor shall include all necessary information to assist with the decision of the MDA program office. Per NISPOM Chapter 7, Section 102c., the Prime Contractor shall act as the focal point for all Subcontractor requests for public release. A lack of response from the MDA program office does not constitute as public release authorization. The Prime Contractor shall not release information to the public prior to receiving written authorization from the MDA program office (this requirement includes any information system that provides public access).

Reference Item 14: Program Protection is required for this contract. The interdisciplinary requirements associated with Program Protection are further addressed in Sections C & J of this contract and detailed in the Government issued Program Protection Plan (PPP). The contractor shall implement applicable security countermeasures to protect classified and/or unclassified Critical Program Information and Critical Components as outlined in the Statement of Work/Performance Work Statement/Statement of Objectives and refined in the PPP.

FOR OFFICIAL USE ONLY/CONTROLLED UNCLASSIFIED INFORMATION SUPPLEMENT

1. Definitions.

a. Controlled Unclassified Information (CUI). Unclassified information which requires access and distribution limitations prior to appropriate coordination and an official determination by cognizant authority approving clearance of the information for release to one or more foreign governments or international organizations, or for official public release. Per DoD Manual 5200.01, Volume 4 it includes the following types of information: "For Official Use Only" (FOUO); "Sensitive But Unclassified" (State Department information); "DEA Sensitive Information" (Drug Enforcement Agency information); "DoD Unclassified Controlled Nuclear Information"; "Sensitive Information" as defined in the Computer Security Act of 1987; and information contained in technical documents (i.e., Technical Data) as discussed in DoD 5230.24, 5230.25, International Traffic in Arms Regulation (ITAR), and the Export Administration Regulations (EAR).

b. Dual Citizenship. A dual citizen is a citizen of two nations. For the purposes of this document, an individual must have taken an action to obtain or retain dual citizenship. Citizenship gained as a result of birth to non-U.S. parents or by birth in a foreign country to U.S. parents thus entitling the individual to become a citizen of another nation does not meet the criteria of this document unless the individual has taken action to claim and to retain such citizenship.

c. For Official Use Only (FOUO). FOUO is a dissemination control applied by the DoD to unclassified information that may be withheld from public disclosure under one or more of the nine exemptions of the Freedom of Information Act (FOIA) (See DOD 5400.7-R). FOUO is not a form of classification to protect U.S. national security interests.

d. National of the United States.Title 8, U.S.C. Section 1101(a)(22), defines a National of the U.S. as:

(1) A citizen of the United States, or,

(2) A person who, but not a citizen of the U.S., owes permanent allegiance to the U.S.

NOTE: 8 U.S.C. Section 1401, paragraphs (a) through (g), lists categories of persons born in and outside the U.S. or its possessions that may qualify as Nationals and Citizens of the U.S. This subsection should be consulted when doubt exists as to whether or not a person can qualify as a National of the U.S.

e. U.S. Person. Any form of business enterprise or entity organized, chartered, or incorporated under the laws of the United States or its possessions and trust territories and any person who is a citizen or national (see National of the United States) of the United States, or permanent resident of the United States under the Immigration and Nationality Act.

2. Access.

a. Access to FOUO/CUI must be limited to U.S. Persons that have a current U.S. security clearance (minimum interim SECRET clearance); or have been the subject of a favorably completed National Agency Check with Inquiries (NACI) or a more stringent personnel security investigation. Access approval by MDA/Special Security is dependent upon completion of a favorable NACI or Contractor equivalent.

(1) Contractor Equivalent: Contractor equivalent includes various background checks such as those performed by employers during hiring process. Minimum checks shall include Citizenship, Personal Identification (Social Security Number), Criminal, and Credit. Contractors shall submit a request for approval on company letter head to MDA/Special Security.

(2) Contractor personnel with dual citizenship that have an active U.S. security clearance (interim Secret or higher) can have access to FOUO/CUI material.

(3) Contractor personnel with dual citizenship that do not have an active U.S. security clearance (interim Secret or higher), the following actions will be completed prior to authorizing access to FOUO/CUI material:

(a) The dual citizen shall surrender the foreign passport to the security office.

(b) The Contractor Company shall provide a signed letter to the dual citizen informing them that if they request their passport be returned to them, or they obtain a new foreign passport, they will be immediately removed from the MDA program. The dual citizen shall acknowledge by signing and dating the letter.

(c) The MDA Program Manager and MDA/Special Security shall be notified and will provide written approval.

b. Non-Sensitive Positions (ADP/IT-III positions). Non-sensitive positions associated with FOUO/CUI are found at Contractor facilities processing such information on their (Contractor's) unclassified computer systems. Personnel nominated to occupy ADP/IT-III designated positions (applies to any individual that may have access to FOUO/CUI on the Contractor's computer system) must have at least a National Agency Check with Inquiries (NACI) or Contractor equivalent (company hiring practices reviewed and approved by MDA/Special Security). When "Contractor equivalent" option is NOT authorized and there is no record of a valid investigation, the Contractor shall contact MDA/Special Security at mdasso@mda.mil, and provide the requested information. MDA/Special Security will assist the Contractor complete the SF85, Position of Trust Questionnaire, and fingerprints.

3. Identification Markings. FOUO/CUI shall be marked in accordance with DoDM 5200.01, Volume 4, Enclosure 3, Section 2.c.

4. Handling. Storage of FOUO/CUI outside of Contractor facilities (i.e. residence, telework facility, hotel, etc.) shall be in a locked room, drawer, filing cabinet, briefcase, or other storage

device. Continuous storage of FOUO/CUI outside of a Contractor facility shall not exceed 30 days unless government approval is granted.

5. Transmission/Dissemination/Reproduction.

a. Subject to compliance with official distribution statements, FOUO markings (e.g., Export Control, Proprietary Data) and/or Non-Disclosure Agreements which may apply to individual items in question; authorized Contractors, consultants and grantees may transmit/disseminate FOUO/CUI information to each other, other DoD Contractors and DoD officials who have a legitimate need to know in connection with any DoD authorized contract, solicitation, program or activity. The government Procuring Contracting Officer (PCO) will confirm with the Contracting Officer's Representative or Task Order Monitor "legitimate need to know" when required. The MDA/Chief Information Officer has determined that encryption of external data transmissions of FOUO/CUI are now practical. The MDA/Chief Information Officer has stated that Public Key Infrastructure (PKI) and Public Key (PK) enabling technologies are available and cost effective. The following general guidelines apply:

(1) In accordance with DoD Manual 5200.01, Volume 4, "Controlled Unclassified Information (CUI)," Enclosure 3, external electronic data transmissions of CUI/FOUO shall be only over secure communications means approved for transmission of such information. Encryption of e-mail to satisfy this requirement shall be in accordance with MDA Directive 8190.01, Electronic Collaboration with Commercial, Educational, and Industrial Partners, May 12, 2009, being accomplished by use of DoD approved Public Key Infrastructure Certification or by the company's participation in the "Federal Bridge."

(2) The MDA/Chief Information Officer (CIO), PKI Common Access Card (CAC) point of Contact is, (b)(6)

b. Failure of the Contractor to encrypt FOUO/CUI introduces significant risks to the BMDS mission. It is essential for the Contractor to understand that mitigation options that are available. The Contractor must understand that failure to encrypt FOUO/CUI carries with it certain risks to the mission. These risks can be mitigated with the thoughtful application of processes, procedures, and technology. Some of the available mitigation tools include:

(1) Approved DoD PKI/CAC hardware token certificates or DoD trusted software certificates for encrypting data in transport.
(2) Industry best practice of Virtual Private Network (VPN) Internet Protocol Security (IPSEC) for intra-organization transport.
(3) Industry best practice of Secure Sockets Layer Portal Web Services for document sharing and storage
(4) Approved DoD standard solutions for encrypting data at rest.
(5) Approved DoD E-Collaboration services via MDA Portal or Defense Information Systems Agency (DISA) Network Centric Enterprise Services (NCES).

(6) Any FIPS 140-2 validated encryption [e.g., IPSEC, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure/Multipurpose Internet Mail Extension (S/MIME).

(7) Procure and employ Secure Telephone Equipment (STE).
(8) Procure and employ secure facsimile (FAX) capability.
(9) Utilize secure VTC capabilities.
(10) Hand-carry FOUO/CUI.
(11) Utilize mailing through U.S. Postal Service.
(12) Utilize overnight express mail services.

c. FOUO/CUI shall be processed and stored internally on Automated Information Systems (AIS) or networks 1) when distribution is to an authorized recipient and 2) if the receiving system is protected by either physical isolation or a password protection system. Holders shall not use general, broadcast, or universal e-mail addresses to distribute FOUO/CUI. Discretionary access control measures may be used to preclude access to FOUO/CUI files by users who are authorized system users, but who are not authorized access to FOUO/CUI. External transmission of FOUO/CUI shall be secured using NIST-validated encryption. FOUO/CUI cannot be placed on any publically-accessible medium.

d. Reproduction of FOUO/CUI may be accomplished on unclassified copiers within designated government or Contractor reproduction areas.

6. Storage. During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO/CUI information unattended where unauthorized personnel are present). After working hours, FOUO/CUI information may be stored in unlocked containers, desks, or cabinets if contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc.

7. Disposition.

a. When no longer required, FOUO/CUI shall be returned to the MDA office that provided the information or destroyed by any of the means approved for the destruction of classified information or by any other means that would make it difficult to recognize or reconstruct the information.

b. Removal of the FOUO/CUI status can only be accomplished by the government originator. The MDA COR shall review and/or coordinate with proper authority the removal of FOUO/CUI status for information in support of contract activity.