Collins Aerospace

HQ0276-15-C-0005_T-SM3 Flowdowns_05-03-2024

U.S. GOVERNMENT CLAUSES

Prime Contract Number: HQ0276-15-C-0005
Date of Creation: 05-03-2024

The following customer contract requirements apply to any Purchase Order referencing the above U.S. Government prime contract number and are hereby incorporated into the Purchase Order by full text or by reference with the same force and effect as if they were given in full text. The terms and conditions of the versions of the "Flowdown of U.S. Government Contract Clauses Under U.S. Government Contracts" and "Flowdown Updates" documents in effect on the date of the particular Order shall also apply. These documents are made available at the RTX Supplier Site. The full text of FAR/DFARS clauses may be accessed at https://www.acquisition.gov/.

In all provisions and clauses listed herein, terms shall be revised to suitably identify the party to establish Supplier's obligations to Buyer and to the Government, and to enable Buyer to meet its obligations under the prime contract. Without limiting the generality of the foregoing, and except where further clarified or modified below, the term "Government" and equivalent phrases shall mean "Buyer", the term "Contracting Officer" shall mean "Buyer's Purchasing Representative", the term "Contractor" or "Offeror" shall mean "Supplier", "Subcontractor" shall mean "Supplier's Subcontractor" under this Purchase Order, and the term "Contract" shall mean this "Purchase Order". For the avoidance of doubt, the words "Government" and "Contracting Officer" do not change: (1) when a right, act, authorization or obligation can be granted or performed only by the Government or the prime contract Contracting Officer or duly authorized representative, such as in FAR 52.227- 1 and FAR 52.227- 2 or (2) when title to property is to be transferred directly to the Government. Supplier shall incorporate into each lower tier contract issued in support of this Purchase Order all applicable FAR and DFARS provisions and clauses in accordance with the flow down requirements specified in such clauses. Nothing in this Purchase Order grants Supplier a direct right of action against the Government. If any of the following FAR or DFARS clauses do not apply to this Purchase Order, such clauses are considered to be self-deleting.

Buyer or Buyer Affiliates reserve the right to add or update any FAR or DFAR clause or special contract provision based on customer contract directives.

Capitalized words used herein and not otherwise defined shall have the meanings ascribed to them in the Terms and Conditions.

The requirements below are in accordance with the U.S. Government prime contract and are not modified by Buyer for each individual Supplier. Supplier will remain at all times responsible for providing to any government agency, Buyer, or Buyer's customer, evidence of compliance with the requirements herein or that such requirements are not applicable to the extent satisfactory to the requesting party.

CLAUSES INCORPORATED BY REFERENCE:

FAR CLAUSES

Clause	Reference
52.219-16	Liquidated Damages – Subcontracting Plan
52.222-3	Convict Labor
52.223-12	Refrigeration Equipment and Air Conditioners
52.229-4	Federal, State, and Local Taxes (State and Local Adjustments)
52.232-8	Discounts for Prompt Payment
52.232-9	Limitation on Withholding of Payments
52.242-1	Notice of Intent to Disallow Costs
52.242-2	Production Progress Reports
52.242-3	Penalties for Unallowable Costs
52.242-4	Certification of Final Indirect Costs
52.243-7	Notification of Changes
52.246-11	Higher-Level Contract Quality Requirement
52.247-68	Report of Shipment (REPSHIP)

DFARS CLAUSES

Clause	Reference
252.203-7000	Requirements Relating to Compensation of Former DoD Officials
252.204-7003	Control of Government Personnel Work Product
252.204-7005	Oral Attestation of Security Responsibilities
252.211-7007	Reporting of Government-Furnished Equipment
252.223.7004	Drug-Free Work Force
252.225-7004	Report of Intended Performance Outside the United States and Canada – Submission After Award
252.225-7010	Levies on Contract Payments

PRIME CONTRACT SPECIAL PROVISIONS

H-09 ORGANIZATIONAL CONFLICT OF INTEREST (Jun 2012)

a. Purpose: The primary purpose of this clause is to aid in ensuring that:

(1) the Contractor's objectivity and judgment are not biased because of its present or planned interests which relate to work under this contract;
(2) the Contractor does not obtain unfair competitive advantage by virtue of its access to non-public information regarding the Government's program plans and actual or anticipated resources; and
(3) the Contractor does not obtain unfair competitive advantage by virtue of its access to proprietary information belonging to others.

b. Scope: Organizational Conflict of Interest (OCI) rules, procedures and responsibilities as described in FAR Subpart 9.5 shall be applicable to this contract and any resulting subcontracts.

(1) The general rules in FAR 9.505-1 through 9.505-4 and the restrictions described herein shall apply to performance or participation by the Contractor and any of its affiliates or their successors-in-interest (hereinafter collectively referred to as "Contractor") in the activities covered by this contract as prime Contractor, subcontractor, co-sponsor, joint venturer, consultant, or in any similar capacity.

(2) The Missile Defense Agency's OCI policy is in Attachment J-14 of this contract.

c. Access to and Use of Nonpublic Information: If the Contractor, in performance of this contract, obtains access to nonpublic information such as plans, policies, reports, studies, financial plans, or data which has not been released or otherwise made available to the public, the Contractor agrees that without prior written approval of the Contracting Officer, it shall not:

(1) use such information for any private purpose;

(2) release such information.

d. Access to and Protection of Proprietary Information: The Contractor agrees to exercise diligent effort to protect proprietary information from misuse or unauthorized disclosure in accordance with the provisions of FAR 9.505-4. The Contractor may be required to enter into a written non-disclosure agreement with the third party asserting proprietary restrictions.

e. Subcontracts: The Contractor shall include this clause in consulting agreements, teaming agreements, subcontracts, or other arrangements for provision of services or supplies of any tier. The terms "contract", "Contractor", and "Contracting Officer" shall be appropriately modified to preserve the Government's rights.

f. Representations and Disclosures:

(1) The Contractor represents that it has disclosed to the Contracting Officer, prior to award, all facts relevant to the existence or potential existence of organizational conflicts of interest as that term is used in FA Subpart 9.5. To facilitate disclosure and Contracting Officer approval, the Contractor shall complete an OCI Defense (BMD), and BMD-related contract or subcontract (form shall be requested from the Procuring Contracting Officer).

(2) The Contractor represents that if it discovers an organizational conflict of interest or potential conflict of interest after award, a prompt and full disclosure shall be made in writing to the Contracting Officer. This disclosure shall include a description of the action the Contractor has taken or proposes to take in order to avoid or mitigate such conflicts.

g. Remedies and Waiver:

(1) For breach of any of the above restrictions or for non-disclosure or misrepresentation of any relevant facts required to be disclosed concerning this contract, the Government may: terminate this contract for default; disqualify the Contractor from subsequent related contractual efforts if necessary to neutralize a resulting organizational conflict of interest; and pursue such other remedies as may be permitted by law or this contract. If, however, in compliance with this clause, the Contractor discovers and promptly reports an organizational conflict of interest (or the potential thereof) subsequent to contract award, the Contracting Officer may terminate this contract for convenience if such termination is deemed to be in the best interest of the Government or take other appropriate actions.

(2) The parties recognize that this clause has potential effects which will survive the performance of this contract and that it is impossible to foresee each circumstance to which it might be applied in the future. Accordingly, the Contractor may at any time seek a waiver from the Director, MDA, (via the Contracting Officer) by submitting a full written description of the requested waiver and the reasons in support thereof.

H-10 ENABLING CLAUSE FOR BMD INTERFACE SUPPORT (APR 2009)

a. It is anticipated that, during the performance of this contract, the Contractor will be required to support Technical Interface/Integration Meetings (TIMS) with other Ballistic Missile Defense (BMD) Contractors and other Government agencies. Appropriate organizational conflicts of interest clauses and additional costs, if any, will be negotiated as needed to protect the rights of the Contractor and the Government.

b. Interface support deals with activities associated with the integration of the requirements of this contract into BMD system plans and the support of key Missile Defense Agency (MDA) program reviews.

c. The Contractor agrees to cooperate with BMD Contractors by providing access to technical matters, provided, however, the Contractor will not be required to provide proprietary information to non-Government entities or personnel in the absence of a non-disclosure agreement between the Contractor and such entities.

d. The Contractor further agrees to include a clause in each subcontract requiring compliance with paragraph c. above, subject to coordination with the Contractor. This agreement does not relieve the Contractor of its responsibility to manage its subcontracts effectively, nor is it intended to establish privity of contract between the Government and such subcontractors.

e. Personnel from BMD Contractors or other Government agencies or Contractors are not authorized to direct the Contractor in any manner.

f. This clause shall not prejudice the Contractor or its subcontractors from negotiating separate organizational conflict of interest agreements with BMD Contractors; however, these agreements shall not restrict any of the Government's rights established pursuant to this clause or any other contract.

H-28 DISTRIBUTION CONTROL OF TECHNICAL INFORMATION (May 2013)

a. The following terms applicable to this clause are defined as follows:

1. DoD Official. Serves in DoD in one of the following positions: Program Director, Deputy Program Director, Program Manager, Deputy Program Manager, Procuring Contracting Officer, Administrative Contracting Officer, or Contracting Officer's Representative.

2. Technical Document. Any recorded information (including software) that conveys scientific and technical information or technical data.

3. Scientific and Technical Information. Communicable knowledge or information resulting from or pertaining to the conduct or management of effort under this contract. (Includes programmatic information).

4. Technical Data. As defined in DFARS 252.227-7013.

b. Except as otherwise set forth in the Contract Data Requirements List (CDRL), DD Form 1423 the distribution of any technical documents prepared under this contract, in any stage of development or completion, is prohibited outside of the contractor and applicable subcontractors under this contract unless authorized by the Contracting Officer in writing. However, distribution of technical data is permissible to DOD officials having a "need to know" in connection with this contract or any other MDA contract provided that the technical data is properly marked according to the terms and conditions of this contract. When there is any doubt as to "need to know" for purposes of this paragraph, the Contracting Officer or the Contracting Officer's Representative will provide direction. Authorization to distribute technical data by the Contracting Officer or the Contracting Officer's Representative does not constitute a warranty of the technical data as it pertains to its accuracy, completeness, or adequacy. The contactor shall distribute this technical data relying on its own corporate best practices and the terms and conditions of this contract. Consequently, the Government assumes no responsibility for the distribution of such technical data nor will the Government have any liability, including third party liability, for such technical data should it be inaccurate, incomplete, improperly marked or otherwise defective. Therefore, such a distribution shall not violate 18 United States Code § 1905.

c. All technical documents prepared under this contract shall be marked with the following distribution statement, warning, and destruction notice: When it is technically not feasible to use the entire WARNING

statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data" required by DoD Directive 5230.25.

1. **DISTRIBUTION** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S. C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoDD 5230.25. Distribution authorized to the DoD and United States (US) DoD Contractors only (critical technology) (30 June 2008). Other requests shall be referred to MDA/AB.

2. **WARNING** - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

3. DESTRUCTION NOTICE - For classified documents follow the procedures in DOD 5220.22-M, National Industrial Security Program Operating Manual, February 2006, Incorporating Change 1, March 28, 2013, Chapter 5, Section 7, or DoDM 5200.01-Volume 3, DoD Information Security Program: Protection of Classified Information, Enclosure 3, Section 17. For controlled unclassified information follow the procedures in DoDM 5200.01-Volume 4, Information Security Program: Controlled Unclassified Information.

d. The Contractor shall insert the substance of this clause, including this paragraph, in all subcontracts.

H-29 COMMERCIAL COMPUTER SOFTWARE LICENSE (Mar 2013)

a. Unless otherwise approved by the PCO, commercial computer software licenses shall, upon delivery and acceptance, designate the U.S. Government as a contingent licensee, able to replace the Contractor as the primary licensee upon notifying the licensor. A copy of the negotiated license shall be furnished to the PCO. The terms of the licenses cannot be inconsistent with Federal procurement law and must satisfy user needs. This includes the Contractor's / subcontractor's needs for the software to perform this contract and the Government's needs for the software to accomplish the Government's ultimate objectives. At a minimum, this shall include the rights to make an archive copy of the software, to relocate the computer on which the software resides, to re-host the software on a different computer, to permit access by support contractors, and to permit the Government to transfer the license to another contractor.

b. Nothing in this clause shall take precedence over any other clause or provision of this contract. Government concurrence, as defined in paragraph a above, does not in any way affect the Government's technical data rights as established by the terms and conditions of this contract.

H-36 CONTRACTOR IDENTIFICATION AND ASSERTION OF RESTRICTIONS ON THE GOVERNMENT'S USE, RELEASE, OR DISCLOSURE OF NON-COMMERCIAL TECHNICAL DATA OR COMPUTER SOFTWARE (DEC 2011)

a. The contractor and its subcontractors shall provide a completed Attachment in accordance with DFARS 252.227-7017 entitled "Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software" that is signed and dated by a responsible official of the Contractor. This Attachment is incorporated herein by reference as if fully set forth. The Attachment identifies and provides information pertaining to technical data (including computer software documentation) and computer software that the contractor and subcontractors claim to qualify for delivery with less than Unlimited Rights. The contractor agrees not to withhold delivery of the technical data or software based on its claims. The Government shall investigate the validity of the contractor's claims and therefore reserves all its rights regarding the technical data/software in question, to include those rights set forth in: DFARS 252.227-7013, Rights in Technical Data - Noncommercial Items; DFARS 252.227-7014, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation; DFARS 252.227-7019, Validation of Asserted Restrictions--Computer Software; DFARS 252.227-7028, Technical Data or Computer Software Previously Delivered To the Government; and, DFAR 252.227-7037, Validation Of Restrictive Markings On Technical Data clauses until a determination is made.

b. The contractor shall have, maintain, and follow written procedures sufficient to assure that restrictive markings/legends are used only when authorized by the terms of this contract and shall maintain records sufficient to justify the validity of any restrictive markings/legends on any technical data or computer software or computer software documentation delivered under this contract. The Contractor agrees that the Government has Unlimited Rights as defined by DFARS 252.227-7013 and 252.227-7014 in any deliverable technical data or computer software or computer software documentation not listed in the Attachment and that such data or software will not be subject to any restrictive markings or legends.

H-42 FOREIGN PERSONS (May 2012)

a. "Foreign National" (also known as Foreign Persons) as used in this clause means any person who is NOT:

1. a citizen or national of the United States; or

2. a lawful permanent resident; or

3. a protected individual as defined by 8 U.S.C.1324b(a)(3). "Lawful permanent resident" is a person having the status of having been lawfully accorded the privilege of residing permanently in the United States as an immigrant in accordance with the immigration laws and such status not having changed.

"Protected individual" is an alien who is lawfully admitted for permanent residence, is granted the status of an alien lawfully admitted for temporary residence under 8 U.S.C.1160(a) or 8 U.S.C.1255a(a)(1), is admitted as a refugee under 8 U.S.C.1157, or is granted asylum under section 8 U.S.C.1158; but does not include (i) an alien who fails to apply for naturalization within six months of the date the alien first becomes eligible (by virtue of period of lawful permanent residence) to apply for naturalization or, if later, within six months after November 6, 1986, and (ii) an alien who has applied on a timely basis, but has not been naturalized as a citizen within 2 years after the date of the application, unless the alien can establish that the alien is actively pursuing naturalization, except that time consumed in the Service's processing the application shall not be counted toward the 2-year period."

c. All employees of all entities that make up the contractor's team, whether subcontractors, consultants, or anyone who works with or on behalf of the contractor will be citizens of the U.S.

H-43 IMPACT OF GOVERNMENT TEAM PARTICIPATION/ACCESS (JUN 2012)

The Government/Contractor organizational/interface approach (e.g., Integrated Product Teams, Team Execution Reviews, Technical Interchange Meetings, and/or Working Groups), will require frequent, close interaction and/or surveillance between the Government and Contractor/subcontractor team members during contract performance. For this purpose the Contractor, recognizing its privity of contract with the Government, authorizes the Government to communicate directly with, and where appropriate visit as well as monitor, the Contractor's subcontractors. This access/interface is necessary to support the Government's quality and program management approach which emphasizes systematic surveillance and evaluation techniques used to assess Contractor /subcontractor performance. Government team members may offer advice, information, support, and facilitate rapid Government feedback on team-related products, provide clarification, and review Contractor/subcontractor progress; however, the responsibility and accountability for successfully accomplishing the requirements of this contract remain solely with the Contractor. Neither the Contractor nor the subcontractor shall construe such advice, surveillance, reviews and clarifications by Government team members as Government-directed changes to the terms of this contract. The PCO is the only individual authorized to direct or approve any change to the terms of this contract.

Have Operations Security (OPSEC) Requirements. The subcontractor is required to apply operations security (OPSEC) to enhance protection of classified and unclassified critical information pursuant to MDA OPSEC Program Instruction 5205.02; DoD OPSEC Program Directive 5205.02; DoD OPSEC Program Manual 5205.02-M; National Security Decision Directive Number 298; 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 A&MDS Industrial Security office for clarification.

Restrict Access to Subcontractor's Unclassified Information System. a) The Subcontractor shall safeguard and protect Covered Defense Information (CDI) 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) and Controlled Technical Data information which resides on, or transits through the subcontractor's (all tiers of subcontracting) unclassified information technology systems. b) The subcontractor shall ensure that all persons accessing CDI, which includes FOUO, meet the qualifications for an Automated Data Processing/Information Technology (ADP/IT)-III Position requirement). c) The "CONTROLLED DEFENSE INFORMATION SUPPLEMENT" provides additional guidance for the handling, marking, transmission, reproduction, safeguarding, and disposition of FOUO/CUI. d) MDA reserves the right to conduct compliance inspections of subcontractor unclassified information systems and other repositories for the protection of CDI.

Markings. Subcontractor shall ensure all material generated under this contract is marked IAW DoD 5220.22-M, National Industrial Security Program Operating Manual, dated 28 February 2006, Incorporating Change 1, dated 28 March 2013. DoDM 5200.01 Vol. 2 DoD Information Security Program, DoD Instruction 5230.24, "Distribution Statements on Technical Documents," and DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure.

Supply Chain Risk Management. a. The Subcontractor shall maintain controls in the provision of supplies and services to the Government to minimize supply chain risk (1.i). b. The Subcontractor shall include the substance of this clause, including this paragraph (12.b.v), in all subcontracts involving the development or delivery of any information technology, whether acquired as a service or as a supply. i. All US domestic suppliers, where applicable, shall demonstrate visibility into the supply chain for LBD by providing an accurate indentured Bill of Material with relevant information pertaining to source of supply. ii. The supply chain shall be required to procure logic bearing devices from the vendors approved by the Defense Microelectronic Activity, during Commercial off-the-Shelf (COTS) refresh/replacement of obsolete parts, or other parts issues as identified by Government SCRM advisories, (Note: If an exception is requested it shall be in writing to the Government COTR and MDA/DEI. This request shall be made via the Raytheon Subcontract Manager with a justification as to why the component could not be procured from a certified vendor). iii. The supplier shall support and participate in unannounced Government audits into their supply chain activities. iv. The supplier shall report discrepancies to the Program Directorate Configuration Review Board via contracts letter to Raytheon Subcontract Manager. v. The supplier shall flow down SCRM requirements to all subcontractors including the value stream, which supply components or have a subsystem design that contains LBD.

Public Disclosure.

1. Proposed public disclosure of unclassified information relating to work under this contract shall be coordinated through the Prime Contractor's Raytheon Subcontract Manager to the MDA COR/TM/CLIN COTR for submission to MDA Public Affairs for public release processing. ONLY information that has been favorably reviewed and authorized by MDA/Public Affairs in writing may be disclosed. Information developed after initial approval for public release must be submitted for re-review and processing. 2. Contemplated visits by public media representatives in reference to this contract shall receive prior approval from the MDA COR/TM/CLIN COTR and from MDA/Public Affairs by submitting requests through the Prime Contractor's Subcontract Manager. 3. Critical technology subject to the provisions of DoD Instruction 5230.24, "Distribution Statements on Technical Documents," and DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," shall be reviewed in accordance with established directives. 4. A request from a foreign government, or representative thereof, including foreign contractors, for classified and/or unclassified information in reference to this contract shall be forwarded to the Prime Contractor's Subcontract Manager for review and appropriate action.

CONTROLLED DEFENSE INFORMATION SUPPLEMENT All subcontractors shall flow all of these requirements through all levels of their supply chain where applicable.

1) Definitions.

a) Automated Information System (AIS). An assembly of computer hardware, software, and firmware configured to automate functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, or textual material.

b) Covered defense information (CDI). Unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—

i) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

iii) 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) and information contained in technical documents (i.e., Controlled Technical Data) as discussed in DoD 5230.24, 5230.25, International Traffic in Arms Regulation (ITAR), and the Export Administration Regulations (EAR).

(1) 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.

iv) Controlled technical information (CTI). Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

(1) Technical Information. Technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013). Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

c) Contractor. In the context of this document means both Prime and Subcontractors throughout the supply chain.

d) 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.

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

i) A citizen of the United States, or,

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

(1) 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.

f) Personal Information. Information about an individual that is intimate or private to the individual, as distinguished from information related to the individual's official functions or public life.

g) 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.

h) Privacy Act. The Privacy Act of 1974, as amended, 5 U.S.C. Section 552a.

i) Supply chain risk: The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a national security system (as that term is defined at 44 U.S.C. 3542(b)) so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. (DFAR 252.239-7017)

j) Supply Chain Risk Management: The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport) (DTM-09-016). The management of risk to the integrity, trustworthiness, and, authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and any other adversarial attempts aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the supply chain. (ICD 731)

k) Logic Bearing Devices (LBD): Microelectronic devices that have the capability to store and process executable code, hash values, or encryption/decryption algorithms.

2. Required Security Requirements Flow Down.

a. In accordance with the prime contract Security Classification Specification (DD Form 254) Reference Item 10.j (For Official Use Only Information), 11.l (Restrict Access to Contractor's Unclassified Automated Information (AIS) and 12 (Public Release), specific requirements for protecting unclassified program information are required to be imposed on all subcontracts. Operational Security (11.j) may be imposed based on subcontractor. The remainder to this supplement discusses these requirements in detail.

3. General.

a. The FOIA requires U.S. Government offices to disclose to any requestor information resident in U.S. Government files unless the information falls under one of nine exemption categories. FOUO/CUI and other information may fall in this category. Mark such information as "For Official Use Only."

b. FOUO/CUI in the hands of subcontractors may not be released to the public by the contractor unless documented written approval has been provided by MDA Public Affairs with concurrence by the COR/TM/CLIN COTR via submission of the request to Raytheon.

4. 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 pending completion of a favorable NACI or Contractor equivalent. The

subcontractor shall submit requests for access for persons maintaining dual citizenship for MDA approval via Raytheon. The subcontractor shall only provide access to FOUO/CUI data once MDA approval is provided via Raytheon.

i. 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 via the Prime Contractor. (Please forward prior MDA/Special Security approvals to the Prime Contractor.)

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

iii. 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:

1. The dual citizen shall surrender the foreign passport to the security office.

2. 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.

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

4. 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.*

5. *Identification* Markings. In accordance with DoD 5200.01 Volume 4; within the Department of Defense CUI shall be marked as FOR OFFICIAL USE ONLY or with a DISTRIBUTION STATEMENT, to include the appropriate WARNING for ITAR or the EAR.

a. An unclassified document that qualifies for FOUO marking, when marked, shall be marked "For Official Use Only" at the top and bottom of the page on the outside of the front cover (if any), on the first page, on each page containing FOUO information, on the back page and on the outside of the back cover (if any), centered at the bottom of the page. For convenience, all pages, even those that do not contain FOUO information, may be marked "For Official Use Only" in documents generated by an automated system.

b. Individual pages within a classified document that contain both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual pages containing FOUO information but no classified information shall be marked "For Official Use Only" at the top and bottom of the page (unless all pages are being marked with the highest overall security classification level).

c. Subjects, titles, and each section, part, paragraph, or similar portion of an FOUO document shall be marked to show that they contain information requiring protection. Use the parenthetical notation “(FOUO)” (or optionally “(U//FOUO)”) to identify information as FOUO for this purpose. Place this notation immediately before the text.

d. All declassified MDA information is “unclassified official government information” and requires official MDA Security and Policy Review prior to official public release. e. E-mails and other electronic files shall be marked in the same fashion as described for documents above, to the maximum extent possible.

6. 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.

7. 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:

b. 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.”.

c. The MDA/Chief Information Officer (CIO), PKI Common Access Card (CAC) point of Contact is, Ms. Ingrid Weecks (719-721-7040). The A&MDS Industrial Security office, PKI Common Access Card (CAC) point of Contact is, Ms. Heather McDowell (520) 794-0305.

d. 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:

i. Approved DOD PKI/CAC hardware token certificates or DOD trusted software certificates for encrypting data in transport
ii. Industry best practice of Virtual Private Network (VPN) Internet Protocol Security (IPSEC) for intra-organization transport
iii. Industry best practice of Secure Sockets Layer Portal Web Services for document sharing and storage
iv. Approved DOD standard solutions for encrypting data at rest

v. Approved DOD E-Collaboration services via MDA Portal or Defense Information Systems Agency (DISA) Network Centric Enterprise Services (NCES)
vi. Any FIPS 140-2 validated encryption [e.g., IPSEC, Secure Socket Layer/Transport Layer Security (SSL/TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME)]
vii. Procure and employ Secure Telephone Equipment (STE)
viii. Procure and employ secure facsimile (FAX) capability
ix. Utilize secure VTC capabilities
x. Hand-carry FOUO/CUI
xi. Utilize mailing through U.S. Postal Service
xii. Utilize overnight express mail services.

e. 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.

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

8. Public Release. All requests for public release, shall be sent through the prime contractor. Contractors must receive written official public release approval for MDA/Ballistic Missile Defense System (BMDS) information from MDA Public Affairs. A lack of response from the MDA program office does not constitute as public release authorization. Contractors shall not release information to the public prior to receiving authorization from the MDA program office (this requirement includes any information system that provides public access)

9. 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.

10. Disposition.

a. When no longer required, FOUO/CUI shall be returned to the MDA office that provided the information, via the STANDARD Missile 3 Program Office 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.