T-SM3 HQ0276-11-C-0002

RAYTHEON MISSILE SYSTEMS
PURCHASE ORDER ATTACHMENT
This attachment is designed for use with awards under Contract HQ0276-11-C-0002

The following Buyer's terms and conditions are revised to include the following additional provisions for this Purchase Order:

52.217-8	Option to Extend Services
52.217-9	Option to Extend the Term of the Contract
52.219-16	Liquidated Damages -- Subcontracting Plan
52.222-3	Convict Labor
52.223-16 Alt1	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products
52.223-14	Toxic Chemical Release Reporting
52.232-9	Limitation on Withholding of Payments
52.242-1	Notice of Intent to Disallow Costs
52.242-3	Penalties for Unallowable Costs
52.242-4	Certification of Final Indirect Costs
52.243-7	Notification of Changes
52.247-68	Report of Shipment (REPSHIP)
252.203-7000	Requirements Relating to Compensation of Former DoD Officials
252.203-7002	Requirement to Inform Employees of Whistleblower Rights
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 in the DoD Item Unique Identification (IUID) Registry
252.215-7002	Cost Estimating System Requirements
252.223-7004	Drug-Free Work Force
252.225-7004	Report of Intended Performance Outside the United States and Canada—Submission after Award
252.232-7010	Levies on Contract Payments
252.239-7000	Protection Against Compromising Emanations
252.239-7001	Information Assurance Contractor Training and Certification
252.251-7000	Ordering From Government Supply Sources

The following additional prime contract requirements are included in this Purchase Order:

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.

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) 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.