T- SACM W15QKN-14-9-1001 DOTC-17-01-INFTO980

RAYTHEON MISSILE SYSTEMS
PURCHASE ORDER ATTACHMENT

This attachment is designed for use with awards under W15QKN-14-9-1001 DOTC-17-01-INFTO980. The following Buyer's terms and conditions are revised to include the following additional provisions for this Purchase Order. The effective version of each clause shall be the same version as that which appears in Buyer's prime contract, or higher-tier subcontract under which this Purchase Order is a subcontract. In all clauses listed herein, terms shall be revised to suitably identify the party to establish Seller'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 "Seller", "Subcontractor" shall mean "Seller's Subcontractor" under this Purchase Order, and the term "Contract" shall mean this "Purchase Order". If any of the following clauses do not apply to this Purchase Order, such clauses are considered to be self-deleting.

ARDEC 18	Physical Security Standards for Sensitive Items
ARDEC 66	Safety Requirements for Hazardous Items
ARDEC 77	Material Safety Data Sheets
ARDEC 169	Explosive Material Handling
ARDEC 68	Identification of Contractor Employees
ARDEC 70	(FOUO) Release of Information Research and Development

The following additional prime contract requirements apply to this Purchase Order:

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

1. The definition of CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding information that is classified pursuant to Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended (References (m) and (n)).

2. When CUI is to be provided to or generated by DoD contractors, the controls and protective measures to be applied shall be described in the pertinent contract documents (e.g., contract clause; statement of work; or DD Form 254, "Department of Defense Contract Security Classification Specification"). Solicitations and contracts shall use a non-disclosure of information clause that prohibits release of unclassified information to the public without approval of the contracting activity.

3. The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract without prior approval from the government.

4. Technical Data is any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictoral delineations in media, such as computer software, drawings, or photographs, text in specifications, or related performance or design documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information, and computer software documentation.

5. GOVERNMENT DISTRIBUTION STATEMENTS: Will be added to all technical data generated during the execution of this contract, in accordance with DoD Directive 5230.24.

6. The contractor shall protect CUI from unauthorized disclosure by appropriately marking, safeguarding, disseminating, and destroying such information.

7. CUI may be identified in security classification guides to ensure the information receives appropriate protection.

8. For unauthorized disclosures of CUI, no formal security inquiry or investigation is required. However, appropriate management action shall be taken to fix responsibility for unauthorized disclosure of CUI whenever feasible or required by other guidance, and appropriate disciplinary action shall be taken against those responsible. The DoD Component that originated the CUI shall be informed of its unauthorized disclosure.

FOR OFFICIAL USE ONLY (FOUO)

1. The "FOR OFFICIAL USE ONLY" marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official government information that may be withheld from the public under exemptions 2 through 9 IAW Army Regulation 25-55, The Department of the Army Freedom of Information Act Program.

2. Control, marking, and protection of FOUO information will be in accordance with this document and Army Regulation 380-5, The Department of the Army Information Security Program, Chapter 5, para 5-1 through 5-6.

3. Specific Handling Instructions: All emails containing (FOUO) will be digitally encrypted in accordance with AR 25-1, para. 6-4 (M-7b.) dated 4 Dec 08.

3. FOR OFFICIAL USE ONLY is restricted to personnel with a valid need to know unless public release authorization has been obtained. Information, in any media format may only be disseminated of FOUO data to those individuals or organizations with direct affiliation with the given program or project. Further dissemination of such information will be at the discretion of the Government Security Manager. Personnel no longer requiring access to FOUO must delete or surrender any in their possession and terminate future access to it. The contractor may disseminate "FOR OFFICIAL USE ONLY" (FOUO) information to their employees who have need to know for the information in connection with this contract.

4. All FOUO material will be destroyed by tearing or shredding to make unreadable. Electroni media will be purged with approved software or destroyed through a physical process.

5. Use of the above marking does not mean that the information cannot be released to the publi only that it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

6. An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if any), on the first page, on each page, on the back, and on the outside of the back cover (if any). No portion marking will be shown.

7. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification of the information appearing on the page. If an individual portion contains FOUO information but no classified information, the page will be marked FOUO.

8. Removal of the "For Official Use Only" marking can only be accomplished by the originator or other competent authority. When the "For Official Use Only" status is terminated, all know holders will be notified to the extent practical.

9. During working hours, "For Official Use Only" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other classified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security is not exercised, locked buildings or rooms will provide adequate after-hours protection or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases. "For Official Use Only" information may be sent via First Class US Mail or by parcel post. Bulky shipments may be set by Fourth Class US Mail.

10. Unauthorized disclosure of "For Official Use Only" information does not constitute a security violation but the Government Customer should be informed of any unauthorized disclosure. The unauthorized disclosure for FOUO information protected by the Privacy Act may result in criminal sanctions.

CAC ACCESS (If applicable):

Specific Handling Instructions: All emails containing (FOUO) will be digitally encrypted in accordance with AR 25-1, para. 6-4 (M-7b.) dated 4 Dec 08.

Access and General Protection/Security Policy and Procedures. Requires the addition of clause:

"All contractor employees, including subcontractor employees, shall comply with all installation and facility access and local security policies and procedures (provided by the Government representative), and security/emergency management exercises. The contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by the installation Provost Marshal Office, Director of Emergency Services, or Security Office. Contractor workforce must comply with all personal identity verification requirements (CFR clause 52.204-9, Personal Identity Verification of Contract Personnel) as directed by DoD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in contractor security matters or processes. During FPCONs Charlie and Delta, services/installation access may be discontinued/postponed due to higher threat. Services will resume when FPCON level and or threat is reduced to an acceptable level as determined by the Installation Commander. Contractor personnel working on an installation are required to participate in the Installation Random Antiterrorism Measures Program as directed. Contractors may be subject to and must comply with vehicle searches, wearing of ID badges, etc"

For contracts involving AA or E applicable to Domestic Violence Amendment to the Gun Control Act of 1968. Requires the addition of: "Contractor must ensure compliance with the Domestic Violence Amendment to the Gun Control Act of 1968 Nothing in this clause shall relieve the Contractor of its responsibility for complying with other applicable Federal, state, and local laws, ordinances, codes, and regulations (including requirements for obtaining licenses and permits) in connection with the performance of this contract."

Threat Awareness Reporting Program. For all contractors with security clearances. Requires the addition of: "Per AR 381-12 Threat Awareness and Reporting Program (TARP), contractor employees must receive annual TARP training by a CI agent or other trainer as specified in 2-4b. This training shall be completed within 12 months after contract start date or effective date of incorporation of this requirement into the contract, whichever applies, and then annually thereafter. The contractor shall submit documentation of completion for each affected contractor employee and subcontractor employee to the COR (or to the contracting officer, if a COR is not assigned) within 14 calendar days after completion of training by all employees and subcontractor personnel." Training can be executed by a local CI agent, online via the Army Learning Management System at https://www.lms.army.mil (and search for TARP), or by contacting the 902nd military intelligence unit at usarmy.picatinny.902-migrp. list.308th-picatinny-fo@mail.mil

Information Management Army Information Technology /IA. Requires the addition of clause: "The Contractor shall be capable of accessing, handling, receiving, and storing UNCLASSIFIED documents, equipment, hardware, and test items, using the applicable standards of FOUO information. All Controlled Unclassified Information (documents designated as FOR OFFICIAL USE ONLY and/or LIMITED DISTRIBUTION) shall be submitted by a controlled means using USPS mail, Safe Access File Exchange (SAFE) website and/or DoD Army approved encryption software as per AR 25-1."

For Official Use Only Information (FOUO) and Controlled Unclassified Information (CUI): Requires the addition of: "Contract personnel shall be capable of accessing, handling, receiving, and storing UNCLASSIFIED documents, equipment, hardware, and test items, using the applicable standards of FOUO and CUI. DFARS Clause 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) applies to this effort."

For Contracts that Involve the Public Release of Information: Requires the addition of clause: "Per AR 530-1, Operations Security, an OPSEC review is required prior to all public releases. All government information intended for public release by a contractor will undergo a government OPSEC review prior to release."

For Official Use Only Information (FOUO) and Controlled Unclassified Information (CUI): The Contractor shall be capable of accessing, handling, receiving, and storing UNCLASSIFIED documents, equipment, hardware, and test items, using the applicable standards of FOUO information. All Controlled Unclassified Information (documents designated as FOR OFFICIAL USE ONLY and/or LIMITED DISTRIBUTION) shall be submitted and electronically transmitted by a controlled means via USPS mail, AMRDEC SAFE website https://safe.amrdec.army.mil/SAFE/ and/or an approved application that is Certified for Networthiness such as the Encryption Wizard.