CUSTOMER CONTRACT REQUIREMENTS
JDAM Compatability Assessment
CUSTOMER CONTRACT 107085-0002-0201-0001

CUSTOMER CONTRACT REQUIREMENTS

The following customer contract requirements apply to this contract to the extent indicated below.

1. Prime Contract Special Provisions The following prime contract special provisions apply to this purchase order

A. Export Control

1. Export Compliance.

Seller agrees to comply with U.S. Export regulations including, but not limited to, the requirements of the Arms Export Control Act, 22 U.S.C. § § 2751-2794, including the International Traffic in Arms Regulation (ITAR), 22 C.F.R. § 120 et seq.; and the Export Administration Act, 50 U.S.C. app. § 2401-2420. Seller is responsible for obtaining from the Government export licenses or other authorizations/approvals, if required, for information or materials provided from one party to another under this Contract. Accordingly, Seller shall not export, directly, or indirectly, any products and/or technology, Confidential Information, Trade Secrets, or Classified and Unclassified Technical Data in violation of any U.S. Export laws or regulations.

2. Export Control Laws/International Traffic in Arms Regulation.

Information Subject to Export Control Laws/International Traffic in Arms Regulation (ITAR): Public Law 90-629, “Arms Export Control Act,” as amended (22 U.S.C 2751 et. Seq.) requires that all unclassified technical data with military application may not be exported lawfully without an approval, authorization, or license under EO 12470 or the Arms Export Control Act and that such data required an approval, authorization, or license for export under EO 12470 or Arms Export Control Act. For purposes of making this determination, the Militarily Critical Technologies List (MCTL) shall be used as general guidance. All documents determined to contain export controlled technical data will be marked with the following notice:

WARNING:

-This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

3. Flow Down.

Seller shall include this Article, suitably modified, to identify all Parties, in all sub-tier subcontracts or other forms of lower tier agreements, regardless of tier.

B. Liability Of The Parties

1. Definitions

For the purposes of this Article the “Parties” is defined as the Government, Buyer’s Customer, Buyer, and Seller.

2. Waiver of Liability

With regard to the activities undertaken pursuant to this Contract, no Party shall make any claim against the others, employees of the others, the others’ related entities (e.g., contractors, subcontractors, etc.), or employees of the others’ related entities for any injury to or death of its own employees or employees of its related entities, or for damage to or loss of its own property or that of its related entities, whether such injury, death, damage or loss arises through negligence or otherwise, except in the case of willful misconduct.

3. Extension of Waiver of Liability

Seller agrees to extend the waiver of liability as set forth above to subcontractors or sub entities at any tier by requiring them, by contract or otherwise, to agree to waive all claims against the Parties.

5. Applicability

Notwithstanding the other provisions of this article, this Waiver of Liability shall not be applicable to:

(i) Claims regarding a material breach or nonpayment of funds;

(ii) Claims for damage caused by willful misconduct; and

(iii) Intellectual property claims.

C. Security

1. Security

Work by Seller under this contract may involve access to Controlled Unclassified Information (CUI) as well as information classified as “Confidential”, “Secret”, or “Top Secret”. Seller and their employees who work on such contracts shall comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operation Manual (DOD 5220.22M), (2) any revisions to that manual that may be issued, and (3) the Agreement security classification specification (DD form 254) if included, and all security requirements including but not limited to OPSEC plans and those security requirements specific to the individual initiatives. During the course of this Contract the Parties may determine that information developed by Seller, Buyer, WDA, and/or the Government pursuant to this Contract shall be treated as classified. Such information shall be classified in accordance with DOD 5220.22M.

(i) If this contract is subsequently modified to include a Contract Security Classification Specification (DD Form 254), Seller must flow down the requirements to all lower tier suppliers.

(ii) If the contract involves a classified effort or involves Controlled Unclassified Information (CUI) effort, the following Department of Defense Directives, ARDEC Clauses, Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS) clauses by reference, and local clauses will be incorporated with the same force and effect as if they were given in full text shall be incorporated into this agreement.

(iii) Specific applicable policies, instructions, and regulations will be identified in each contract. Throughout the life of the contract, if any policy, instruction, or regulation is replaced or superseded, the replacement or superseding version shall apply, and shall be subject to the Changes clause of this Contract. The following is a snapshot of key regulatory documents, policies, regulations, etc. applicable at time of award.

(a) DoD 5200.01DoD Information Security Regulation, 24 Feb 12

(b) DoD 5200.2-R Personnel Security Regulation, Jan 87

(c) DoDD 5220.22 National Industrial Security Program, 28 Feb 06

(d) DoDI 5200.01 Vol 4, Information Security Program and Protection of Sensitive Compartmented Information, 24 Feb 12

(e) DoD 5400.7-R, DOD Freedom of Information Act, Sept 98

(f) DODD 2000.12, Antiterrorism Program, 18 Aug 03

(g) ARDEC Clause 68, Identification of Contractor Employees (requirement is only applicable to contractor employees working on Picatinny Arsenal)

(h) ARDEC Clause 18, Physical Security Standards for Sensitive Items (Required when AA&E apply)

(i) ARDEC Clause 70, (FOUO) Release of Information Research and Development (reference FAR 2.101)

(j) FAR Clause 4.402, Safeguarding Classified Information Within Industry

(k) FAR Clause 52.204-2, Security Requirements, Aug 1996

2. Agreement Structure

Upon contract completion or termination, Seller must:

(a) Return ALL classified received or generated under the contract;

(b) Destroy all of the classified; or,

(c) Request retention for a specified period of time

In all subcontracts, lower tier agreements, regardless of tier, the following statement shall be flowed down unless otherwise stated within the contract.

Classification guidance for requirement – "The security level for this agreement is UNCLASSIFIED."

D. Other Requirements

1. For Contracts that Involve the Public Release of Information. Per or DoDM 5205.02-M, an OPSEC review is required prior to all public releases. All government information intended for public release by a subcontractor will undergo a WDA and government OPSEC review prior to release.

2. For Official Use Only Information (FOUO) and Controlled Unclassified Information (CUI). Seller 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.

3. iWATCH (See Something, Say Something) Training. All Seller and Seller subcontractor employees, including lower tier subcontractor employees, shall receive training and participate in the local iWATCH program. This locally developed training will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity to their security officer. This training shall be completed within 45 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies, and then annually thereafter. Seller shall submit certificates of completion for each affected Seller or Seller subcontractor employee and lower tier subcontractor employee to Buyer within 14 calendar days after completion of training by all employees and lower tier subcontractor personnel.

E. Safeguarding Covered Defense Information And Cyber Incident Reporting

If Covered Defense Information (CDI) is identified at the contract level and Seller will (a) on its enterprise level information systems, implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 not later than December 31, 2017 per the requirements of Interim Rule DFARS Clause 252.204-7012 (DEC 2015), and (b) make reasonable best efforts regarding the same for those other areas still requiring analysis, specifically Seller's program unique systems/ tools and subcontracts requiring flowdown, as applicable. After completion of such additional analysis, Seller shall notify the DoD Chief Information Officer within 30 days of contract award of the standards which are currently not in compliance at the time of award, and immediately thereafter of any additional security requirements which have not been implemented. Seller shall provide written confirmation to Buyer that the required notification to the DoD Chief Information Officer has been completed. Seller will implement such security requirements as do not drive adverse cost or schedule impact. Implementation of requirements that will result in adverse impacts to cost or schedule shall be addressed at the government's discretion by equitable adjustment through Buyer. Nothing in this paragraph shall be interpreted to foreclose Seller's right to seek alternate means of complying with the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (as contemplated in DFARS 252.204-7008 (Compliance with Safeguarding Covered Defense Information Controls) and/or DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)).