CUSTOMER CONTRACT REQUIREMENTS
FY15 MINOTAUR SUPPORT
CUSTOMER CONTRACT P000008804

CUSTOMER CONTRACT REQUIREMENTS

The following customer contract requirements apply to this contract to the extent indicated below. If this contract is for the procurement of commercial items under a Government prime contract, as defined in FAR Part 2.101, see Section 3 below.

1. FAR Clauses The following contract clauses are incorporated by reference from the Federal Acquisition Regulation and apply to the extent indicated. In all of the following clauses, "Contractor" and "Offeror" mean Seller.

52.203-13 Contractor Code of Business Ethics and Conduct (APR 2010). This clause applies only if this contract is in excess of $5,000,000 and has a period of performance of more than 120 days.

52.219-8 Utilization of Small Business Concerns (OCT 2014).

52.222-17 Nondisplacement of Qualified Workers (MAY 2014). The term “Contracting Officer” shall mean “Buyer” in paragraph (d)(1). In paragraph (d)(1), “30 days” is changed to “40 days” and “10 days” is changed to “15 days.”

52.222-26 Equal Opportunity (MAR 2007).

52.222-35 Equal Opportunity for Veterans. (JUL 2014). This clause applies only if this contract is $100,000 or more.

52.222-36 Equal Opportunity for Workers with Disabilities (JUL 2014). This clause applies only if this contract exceeds $15,000.

52.222-40 Notification of Employee Rights Under the National Labor Relations Act. (DEC 2010).

52.222-50 Combating Trafficking in Persons (FEB 2009). In paragraph (d), the term "Contracting Officer" means Buyer, and in paragraph (e), the term "the Government" means Buyer.

2. DoD FAR Supplement Clauses DoD Contracts. The following contract clauses are incorporated by reference from the Department of Defense Federal Acquisition Regulation Supplement and apply to the extent indicated. In all of the following clauses, "Contractor" and "Offeror" mean Seller except as otherwise noted.

252.239-7018 Supply Chain Risk (NOV 2013). This clause applies to all contracts involving the development or delivery of any information technology, whether acquired as a service or as a supply.

252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (MAY 2014). This clause applies to contracts for electronic parts or assemblies containing electronic parts or for contracts for the performance of authentication testing. The term "Contractor" means "Buyer" in the first sentence. In paragraph (c)(6), "Contracting Officer" means "Buyer."

252.247-7023 Transportation of Supplies by Sea-Basic (APR 2014). This clause applies if this contract is for supplies that are of a type described in paragraph (b)(2) of this clause. In paragraph (d), "45 days" is changed to "60 days." If this contract exceeds the simplified acquisition threshold, paragraphs (a)-(h) apply. In paragraph (g) "Government" means Buyer. If this contract is at or below the simplified acquisition threshold, paragraphs (f) and (g) are excluded.

252.247-7024 Notification of Transportation of Supplies by Sea (MAR 2000). Contracting Officer and, in the first sentence of paragraph (a), Contractor mean Buyer. This clause applies only if the supplies being transported are noncommercial items or

commercial items that (i) Seller is reselling or distributing to the Government without adding value (generally, Seller does not add value to items that it contracts for f.o.b. destination shipment); (ii) are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or (iii) are commissary or exchange cargoes transported outside the Defense Transportation System in accordance with 10 U.S.C. 2643.

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

Special Provisions .

CONFLICT OF INTEREST

The Seller warrants that, to the best of the Seller's knowledge and belief, there are no relevant facts or Circumstances at the time of the execution of this subcontract which could give rise to an Organizational Conflict of Interest (OCI) as defined in FAR 9.5.

The Seller agrees that if an actual or potential OCI is discovered after award, the Seller shall make a full disclosure in writing to the Buyer. This disclosure shall include a description of actions which the Seller has taken or proposes to take, after consultation with the Buyer, to avoid, mitigate, or neutralize the actual or potential conflict.

The Buyer, may terminate this Agreement, in whole or in part, if it deems such termination necessary only if OCI cannot be mitigated. If the Seller knew of an OCI prior to award, or discovered an actual or potential conflict after award, and did not disclose or misrepresented relevant information to the Buyer, the Buyer may terminate the Agreement for default, or pursue such other remedies as may be permitted by law, regulation (including the FAR and its supplements), or this Agreement.

The Seller shall include this provision, including this paragraph, in subcontracts of any tier which involve access to information covered by this provision.

CYBERSECURITY

The Seller shall provide adequate security to safeguard Buyer and Customer information/data on its information systems from unauthorized access and disclosure. The Seller shall apply the following basic safeguarding requirements to Buyer and Customer information/data:

1) Protecting Buyer and Customer information on public computers or websites. It is prohibited to process Buyer and Customer information/data on public computers (e.g., those available for use by the general public in kiosks, hotel business centers, etc.) or computers that do not have access control. Buyer and Customer information/data shall not be posted on websites that are publicly available or have access limited only by domain/Internet Protocol restriction. Such information may be posted to web pages that control access by user ID/password, user certificates, or other technical means, and that provide protection via use of security technologies. Access control may be provided by the intranet (vice the website itself or the application it hosts).

2) Transmitting electronic information. Transmit email, text messages, blogs, and similar communications using technology and processes that provide appropriate levels of security and privacy, given facilities, conditions, and environment.

3) Transmitting voice and fax information. Transmit voice and fax information only when the sender has a reasonable assurance that access is limited to authorized recipients.

4) Physical or electronic barriers. Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

5) Sanitization. At a minimum, clear information/data on media that has been used to process Buyer and Customer information/data before external release or disposal. Overwriting is an acceptable means of clearing media in accordance with National Institute of Standards and Technology 800-88, Guidelines for
Media Sanitization, at http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

6) Intrusion protection. Exercise reasonable care against computer intrusions and data compromise including exfiltration by adopting appropriate measures including the following:

a. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.
b. Prompt application of security relevant software upgrades, e.g., patches, service packs, and hot fixes.

7) Transfer imitations. Transfer Buyer and Customer information only to those second tier subcontractors that both have a need to know and provide at least the same level of security as specified in this clause.

By executing this agreement, Seller certifies and affirms that the controls and requirements in this clause are in place. The Seller also certifies and affirms that they will immediately contact Buyer if there are any internal or external violations of their information systems.