ISLAND CITY

Section D: Required Subcontractor flow-down clauses specific to LEUT CONTRACT W56HZV16R0210
Revised: June 28, 2018 in addition to contractual clauses contained Sections: A, B and Section C Certifications

---

C.5.1 Configuration Management (CM). The subcontractor shall implement a CM program for configuration planning, identification, control, status accounting, verification, audit, and data management of the Type II LEUT and document the CM program in a CM Plan. To maximize return on investment and reduce life cycle costs, the subcontractor shall use best practices to implement the technical and program management principles fundamental to CM detailed in C.5.1.1 below. The subcontractor shall deliver the CM Plan IAW CDRL A005.

C.5.1.1 Configuration Management Standards. The subcontractor shall perform CM as required by this contract and as extracted from the SAEEIA-649-1, Configuration Management Requirements for Defense Contracts. SAE GEIA-HB-649, Implementation Guide for CM, may be used for guidance.

C.5.2 Configuration Identification and Data Management (DM). The subcontractor shall perform data management, provide the configuration documentation to document the physical and functional characteristics of the Type II LEUT, establish baselines for configuration control, and assign product and document identifiers as required by sections C.3.3, C. 5.2.1, C.5.2.2, C.5.2.3, C.5.2.4, and C.5.2.3.1. The subcontractor is responsible for all original data in its possession, including drawings, models, and associated documents. The subcontractor shall flow down CM and DM requirements to subcontractors and suppliers to provide an appropriate application of CM and DM functions and principles to the entire supply chain.

C.5.2.1 Data Management. The subcontractor shall possess an authoritative product data, engineering or configuration management system and the processes to effectively manage, securely store, release, validate, and track multiple versions and iterations of the Type II LEUT: as-designed, as-integrated, as-built, and as-delivered configuration baselines; this includes management of product structures, product definition documents and data, subcontractor test and analysis data, GFI and other related technical documents.

C.5.2.2 Version Control and Traceability. The subcontractor shall assign a unique identifier to product data and utilize disciplined version control in managing digital data. Each revision (version) shall be a new master, and the subcontractor shall retain all approved revisions of each document and model representation to provide a traceable history in order to access the correct revision when needed. Numerical revisions are not allowed. The subcontractor shall ensure that all representations (i.e., Adobe PDF, CAD, etc.) of a single version or revision of data, delivered to the Government for approval and subsequently maintained by the subcontractor for the term of this contract, are identical. The content of a document and model revision is fixed once approved by PD LTV.

C.5.2.3 Configuration Baseline and Release. The subcontractor shall have a process in place for initial release of design information, release of approved changes to the design information, and delivery of released data to the Government. The subcontractor shall be responsible for creating and maintaining the design release configuration (e.g., developmental baseline, design release baseline) up to date, by incrementally releasing new design data and incorporating approved engineering changes to the Type II LEUT design as they occur. The subcontractor shall maintain an up to date incremental developmental baseline for the Type II LEUT. At completion of the CDR, the subcontractor shall establish and maintain the Initial Product Baseline (IPBL) (e.g., initial production configuration baseline). This IPBL shall identify and document the functional and physical characteristics of the Type II LEUT. The design release configuration shall then be incrementally updated to incorporate approved changes resulting in a Final Product Baseline (FPBL) as an output of PQT approval, Logistics Demonstration, PRR, and Physical Configuration Audit (PCA). The subcontractor shall maintain an updated product baseline for the entire period of performance and submit the IBOM IAW CDRL A047.

C.5.2.3.1 Design Freeze for Test. The Type II LEUT design shall be frozen upon delivery of the first test asset(s) to the test site; all test assets delivered shall be identical in configuration. The subcontractor shall not incorporate changes without prior Government approval.

C.5.2.4 Product and Enterprise identifiers. The Part or Identifying Number (PIN), in combination with the Commercial and Government Entity (CAGE), establishes unique item identification of products. A PIN and CAGE shall be used to uniquely identify all Type II LEUT products. The Government is the design activity (i.e., design authority, customer, procuring activity) for all products (e.g., hardware, software, models, drawings, associated documents) newly developed, or altered or modified from already developed products. The subcontractor shall assign a Government PIN for the product identifier when TACOM is the design activity, assigning CAGE 19207 as the enterprise identifier. Design documents (e.g., CAD models, drawings) for new or modified or altered items shall be numbered the same as, or included within, the part number.

C.16 SECURITY REQUIREMENTS.

C.16.1 The contract will not require access to classified information in performance of this contract. The subcontractor will have access to Controlled Unclassified Information (CUI). CUI is unclassified information requiring application of access, distribution controls, and protective measures which meets the standards for safeguarding and dissemination controls pursuant to statute, and Government-wide policies under Executive Order (EO) 13556. The types of information considered CUI for the program are technical data and information marked Unclassified//For Official Use Only (U//FOUO). 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. When handling U//FOUO information, the subcontractor shall adhere to the following guidelines, the DoDM 5200.01, Army Regulation (AR) 25-55, AR 25-2, and AR 25-1. The procedures for the protection of CUI are as outlined in the Controlled Unclassified Information (CUI) attachment (Attachment 0023).

C.16.1.1 The subcontractor shall not transmit any U//FOUO information electronically over the Internet unless it is encrypted by Federal Information Processing Standard (FIPS) 140-2 standard encryption. In order to enable e-mail encryption the subcontractor shall have or obtain ECA Certificates or Federated Bridge Certificates. Details on the ECA program and authorized ECA vendors can be found at: http://iase.disa.mil/pki/eca/ and details on the Federated bridge program can be found at: http://iase.disa.mil/pkipke/interoperability/Pages/index.aspx .

C.16.2 OPSEC Standard Operating Procedure or Plan. The subcontractor shall follow the Joint Program Office Joint Light Tactical Vehicle (JPO JLTV) OPSEC Plan, dated 27 February 2017 (Attachment 0022), as well as annexes and updates. The subcontractor is not required to develop their own OPSEC Plan. All U.S. subcontractors shall provide annual Program specific OPSEC training for all Program personnel. New Program personnel shall receive JPO JLTV OPSEC Plan specific training within 30 days of Program assignment. Annually, subcontractors shall complete OPSEC training and submit a report, validating 100% completion to the Government Contracting Office by 30 September. These requirements, OPSEC Plan and training, shall be flowed down to all U.S. subcontractors with access to CUI material.

The subcontractor shall develop and submit an Annex, IAW CDRL A035, to the JPO JLTV OPSEC Plan. The subcontractor Annex shall identify information specific to the subcontractor or subcontractor location that is not addressed in the government's plan and document countermeasures not identified in the government's OPSEC Plan.

C.16.3 Operations Security (OPSEC). If the subcontractor generates unclassified OPSEC sensitive information, this information will be protected at the same level as U//FOUO information. The subcontractor shall be responsible for the development of an OPSEC program, IAW DoDM 5205.02-M and AR 530-1, with specific features based on command or unit approved OPSEC requirements.

C.16.3.1 Because of antiterrorism/force protection, operations security, and counterintelligence concerns, the subcontractor shall not release any Controlled Unclassified Information (CUI)/FOUO diagrams, maps, floor plans, schematics, or digital pictures of any installations to foreign Governments, outside organizations or companies without the approval of the COR and G2-TACOM LCMC. All information proposed for public release in any form (video, pictures, article, brochure, website) will undergo a Program Executive Office (PEO) Combat Support and Combat Service Support (CS&CSS) OPSEC Review using the most current and approved PEO CS&CSS STA Form 7114.

C.16.3.2 Examples of information that would be considered OPSEC sensitive: Equipment capabilities, limitations, and vulnerabilities; Detailed mission statements; Operation schedules; Readiness and vulnerability assessments; Test locations and dates; Inventory charts and reports; Detailed budget data; Photographs of components; Detailed organizational charts (with phones and e-mail listings); Technical and scientific data; Unclassified technical data with military applications; Critical maintenance information; Information extracted from a DOD Intranet web site; Lessons learned that could reveal sensitive military operations, exercises, or vulnerabilities; Logistics support (munitions, weapons, movement); Specific real time support to current or on-going military operations; Delivery schedules; and Manufacturing methods.

C.16.4 Protection and Disclosure of Government Information - Public Release Requests. Except for information previously approved for public release by the Government, the subcontractor shall not release any information regarding the work performed under this contract outside (i) the United States Government, (ii) its own facility, (iii) its subcontractors performing Type II LEUT work at any tier, (iv) Associate subcontractors, at any tier, and (v) any other individual or entity that is not contractually bound to protect Information from public release without first obtaining approval for Public Release. Refer to the Joint Program Office Joint Light Tactical Vehicle (JPO JLTV) Security Classification Guide (SCG) (Attachment 0024, section 7) on public release of information for additional guidance. The SCG also provides instructions and guidance on the classification and declassification of information and material pertaining to the JPO JLTV.

The subcontractor shall screen all information submitted for determination of public release to ensure it is both unclassified and technically accurate. A letter of transmittal must certify the review. Program information shall not be released outside program channels IAW Distribution Statements until the review process is complete. Type II LEUT information is any Program information on the Type II LEUT effort. Refer to the JPO JLTV SCG (Attachment 0024) on public release of information for additional guidance. All requests shall be submitted through the PCO for adjudication. The program requires 45 working days to process the request and render a decision.

The subcontractor shall submit all requests for public release approval through the PCO for review by a Government technical and Security personnel, culminating in a determination by the Government Public Affairs Officer (PAO) IAW DFARS 252.204-7000. The PAO will, after appropriate review, either authorize or reject the request to disseminate Government information publicly. Note that authorization may be given contingent on specified changes being made to the material for which public release has been requested. Requests for public release shall be sent electronically via encrypted email using cryptographic products that are National Institute for Standards and Technology/National Information Assurance Partnership (NIST/NIAP) approved or mail the Compact Disc/Digital Video Disc (CD/DVD) using U.S. Postal Service Registered Mail.

C.16.5 Release of Information. The subcontractor shall not release any information or data to third parties without the express written approval of the PCO.

C.16.6 Information Flow Down. The subcontractor shall ensure the security requirements and guidelines contained in section C.16, the program Operations Security (OPSEC) Requirements contained in section C.16.3, and CUI instruction contained in section C.16.4, are contractually flowed down to subcontractors, teammates and consultants.

C.16.7 Common Access Card (CAC) and Installation Access Identification.

C.16.7.1 All subcontractor employees requiring access to the Detroit Arsenal (DTA) for more than a six month period will be sponsored for a Detroit Arsenal Identification card by the COR. Subcontractor employees requiring access to DoD computer networks and systems or traveling OCONUS shall be issued a CAC. More information on the CAC can be found at http://www.cac.mil/common-access-card/getting-your-cac/forcontractors/.

C.16.7.2 The subcontractor shall properly protect and handle Identification (ID) Cards and report lost or stolen cards. For CAC, refer to http://www.cac.mil/common-access-card/getting-your-cac/managing-your-cac/ . For the DTA, the proper identification or badge shall be displayed while on the installation on the front of the outer garment between the shoulder and waist. The subcontractor is responsible for ensuring all ID cards are properly safeguarded and accounted for at all times. The subcontractor shall file a Detroit Arsenal Police report in cases of loss, theft, forgery, or damage.

C.16.7.3 The subcontractor shall ensure that all employees, including all subcontractor employees at all tiers, return installation and access badges IAW FAR 52.204-9 to the Visitor Control Center for deactivation and destruction according to the approved policies. If a subcontractor employees badge is not returned, the subcontractor shall report the unrecovered badge to the Detroit Arsenal Police. Subcontractor employees in possession of a CAC shall be responsible for turning in the CAC IAW FAR 52.204-9 and Local Clause 52.204-4600. All ID cards (installation or CAC) are property of the U.S. Government and shall be returned upon separation, resignation, firing, termination of contract or affiliation with the DoD, or upon any other event in which the individual no longer requires the use of an ID card.