

## **JLTV Flowdowns and Contract Clauses**

Below are the Prime Contract provisions which Buyer has determined either (a) are required to be flowed down to subcontractors under the terms of the Prime Contract; or (b) are necessary to ensure Buyer remains compliant with its obligations to Customer under the Prime Contract. Seller shall comply with each of the provisions below which applies to the Goods or Services, or any of the work performed by Seller under the Order. In addition, Seller agrees to comply with Prime Contract requirements not otherwise stated herein if those requirements are (1) applicable to the Goods or Service furnished by Seller under this Order and (2) are necessary for Buyer to comply with its obligations to Customer. The following modifications are made to the specific terms herein:

Where the words “Contracting Officer” and “Contractor” appear in the text of such provisions, such reference shall mean “Buyer” and “Seller,” respectively. References in such provisions to the “Government,” the United States Department of Defense (“DoD”), “agency,” or such other similar governmental entity shall mean “Buyer,” unless it is clear that the obligation at issue flows to the U.S. Government, in which case the meaning of the terms “Government,” “DoD,” or like terms shall remain the same. The term “subcontractor” shall refer to any lower-tiered subcontractors retained by Seller. All references in such provisions to “Contract” or similar such terms (i.e. “contract vehicle,” etc.) shall mean the Order. If any Prime Contract provision requires Buyer to file a response, report, or claim within a specified period and such response or claim is on behalf of, in conjunction with, or in any way based on information or data to be provided by, Seller, Seller shall submit any relevant information, evidence, or data related to such response or claim to Buyer within the first one-half of such specified period. References in any provision incorporated by reference herein to the “Disputes” clause shall be construed as references to the “Disputes” provision contained elsewhere in the Order. No provision herein shall be taken to imply any direct access on the part of the Seller to the Disputes process as defined in the terms of the Prime Contract.

Unless expressly stated otherwise herein, if any Prime Contract provision requires Buyer to file a response, report, or claim within a specified period and such response or claim is on behalf of, in conjunction with, or in any way based on information or data to be provided by, Seller, Seller shall submit any relevant information, evidence, or data related to such response or claim to Buyer within the first one-half of such specified period.

Capitalized terms used above but not otherwise defined herein have the meanings given to them in AM General LLC JLTV Supplier Term and Conditions of Purchase.

## **FAR and DFAR Clauses**

<b>Clause</b>	<b>Title</b>	<b>Date</b>
52.203-6	Restrictions on Subcontractor Sales to the Government	JUN 2020
52.203-7	Anti-Kickback Procedures	JUN 2020
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	JUN 2020
52.203-13	Contractor Code of Business Ethics and Conduct	NOV 2021
52.203-15	Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Section 1553 of Pub. L. 111-5) (if the subcontract is funded under the Recovery Act)	JUN 2010
52.203-16	Preventing Personal Conflicts of Interest (if supplier performs acquisition functions closely related with inherently governmental function)	JUN 2020

<b>Clause</b>	<b>Title</b>	<b>Date</b>
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-2	Security Requirements	MAR 2021
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-21	Basic Safeguarding of Covered Contractor Information Systems (other than subcontracts for commercially available off-the-shelf items)	NOV 2021
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	NOV 2021
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	NOV 2021
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	NOV 2021
52.211-5	Material Requirements	AUG 2000
52.211-15	Defense Priority and Allocation Requirements	APR 2008
52.215-2	Audit and Records – Negotiation	JUN 2020
52.215-13	Subcontractor Certified Cost or Pricing Data – Modifications (DEVIATION 2022-O0001) (if subcontract greater than \$2M)	APR 2021
52.215-15	Pension Adjustments and Asset Reversions (if cost or pricing data required)	OCT 2010
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions (if cost or pricing data required)	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-23	Limitations on Pass-Through Charges	JUN 2020
52.219-8	Utilization of Small Business Concerns (15 U.S.C.637(d)(2) and (3)) (if the subcontract offers further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities).	OCT 2022
52.219-9	Small Business Subcontracting Plan (if subcontract > \$750k, unless small business)	OCT 2022
52.222-1	Notice to the Government of Labor Disputes	FEB 1997
52.222-19	Child Labor—Cooperation with Authorities and Remedies (Deviation 2020-O0019)	JAN 2022
52.222-21	Prohibition of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	SEP 2016
52.222-35	Equal Opportunity for Veterans	JUN 2020
52.222-36	Equal Opportunity for Workers with Disabilities	JUN 2020
52.222-37	Employment Reports on Veterans	JUN 2020
52.222-40	Notification of Employee Rights Under the National Labor Relations Act (E.O. 13496)	DEC 2010
52.222-50	Combating Trafficking in Persons	NOV 2021
52.222-54	Employment Eligibility Verification	MAY 2022

Clause	Title	Date
52.222-55	Minimum Wages for Contractor Workers under Executive Order 14026 (subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute)	JAN 2022
52.222-62	Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706) (if subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute)	JAN 2022
52.223-3	Hazardous Material Identification and Material Safety Data	FEB 2021
52.223-11	Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons	JUN 2016
52.223-7	Notice of Radioactive Materials* <ul style="list-style-type: none"> <li>Insert “60 days” in the blank space set forth in the first sentence of Paragraph (a) of FAR 52.223-7.</li> </ul>	JAN 1997
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	JUN 2020
52.224-3	Privacy Training (5 U.S.C. 552a)	JAN 2017
52.225-13	Restrictions on Certain Foreign Purchases	FEB 2021
52.225-26	Contractors Performing Private Security Functions Outside the United States	JAN 2025
52.227-1	Authorization and Consent	JUN 2020
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	JUN 2020
52.227-6	Royalty Information	APR 1984
52.227-10	Filing of Patent Applications – Classified Subject Matter	DEC 2007
52.230-2	Cost Accounting Standards	JUN 2020
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors (if supplier is a small business)	NOV 2021
52.234-1	Industrial Resources Developed Under Defense Production Act Title III	SEP 2016
52.244-6	Subcontracts for Commercial Products and Services	OCT 2022
52.245-1	Government Property	SEP 2021
52.251-1	Government Supply Sources	APR 2012
52.247-63	Preference for U.S.-Flag Air Carriers	JUN 2003
52.247-64	Preference for Privately Owned U.S.-Flag Commercial Vessels (if flow down is required in accordance with paragraph (d) of FAR 52.247-64)	NOV 2021
52.248-1	Value Engineering	JUN 2020
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.204-7000	Disclosure of Information	OCT 2016
252.204-7004	Antiterrorism Awareness Training for Contractors	FEB 2019
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	JAN 2025
252.204-7015	Notice of Authorized Disclosure of Information for Litigation Support	MAY 2016

<b>Clause</b>	<b>Title</b>	<b>Date</b>
252.204-7018	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services	JAN 2021
252.204-7020	NIST SP 800-171 DoD Assessment Requirements	MAR 2022
252.211-7003	Item Unique Identification and Valuation	MAR 2022
252.219-7004	Small Business Subcontracting Plan (Test Program) (if supplier participates in Test Program)	MAY 2019
252.223-7001	Hazard Warning Labels	DEC 1991
252.223-7006	Prohibition on Storage, Treatment, and Disposal of Toxic and Hazardous Materials – Basic	SEP 2014
252.223-7008	Prohibition of Hexavalent Chromium	JUN 2013
252.225-7007	Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies (if subcontract is for items covered by USML or 600 series of CCL)	DEC 2018
252.225-7009	Restriction on Acquisition of Certain Articles Containing Specialty Metals (exclude and reserve paragraph (d) and (e)(1))	DEC 2019
252.225-7012	Preference for Certain Domestic Commodities	APR 2022
252.225-7013	Duty-Free Entry	MAR 2022
252.225-7015	Restriction on Acquisition of Hand or Measuring Tools	JUN 2005
252.225-7021	Trade Agreements – Basic (Deviation 2020-O0019)	MAR 2022
252.225-7030	Restriction on Acquisition of Carbon, Alloy, and Armor Steel Plate	DEC 2006
252.225-7033	Waiver of United Kingdom Levies (if supplier is a UK firm)	APR 2003
252.225-7048	Export-Controlled Items	JUN 2013
252.225-7052	Restriction on the Acquisition of Certain Magnets, Tantalum, and Tungsten	AUG 2022
252.226-7001	Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	APR 2019
252.227-7015	Technical Data – Commercial Items	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions – Computer Software	SEP 2016
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends	MAY 2013
252.227-7037	Validation of Restrictive Markings on Technical Data	APR 2022
252.227-7039	Patents—Reporting of Subject Inventions	APR 1990
252.227-7038	Patent Rights – Ownership by the Contractor (Large Business)	JUN 2012
252.229-7011	Reporting of Foreign Taxes – U.S. Assistance Programs	SEP 2005
252.232-7017	Accelerating Payments to Small Business Subcontractors – Prohibition on Fees and Consideration (if supplier is a small business)	APR 2020
252.234-7002	Earned Value Management System (DEVIATION 2015-O0017)	SEP 2015
252.234-7004	Cost and Software Data Reporting System – BASIC	NOV 2014
252.235-7003	Frequency Authorization - Basic	MAR 2014
252.239-7018	Supply Chain Risk (Deviation 2018-O0020)	SEP 2018
252.244-7000	Subcontracts for Commercial Items	JAN 2021
252.245-7001	Tagging, Labeling, and Marking of Government-Furnished Property	APR 2012
252.245-7002	Reporting Loss of Government Property	JAN 2021

<b>Clause</b>	<b>Title</b>	<b>Date</b>
252.246-7003	Notification of Potential Safety Issues	JUN 2013
252.246-7007	Contractor Counterfeit Electronic Part Detection and Avoidance System	AUG 2016
252.246-7008	Sources of Electronic Parts (unless supplier is the original manufacturer)	MAY 2018
252.247-7023	Transportation of Supplies by Sea – Basic	FEB 2019
252.249-7002	Notification of Anticipated Contract Termination or Reduction	JUN 2020
252.251-7000	Ordering From Government Supply Sources	AUG 2012

The following clauses shall apply in addition to those above for Orders that are exclusively for Goods or Service that are not commercial products or commercial services. Commercial products or commercial services, as used herein, shall have the same meaning given to those terms under FAR 2.101.

<b>Clause</b>	<b>Title</b>	<b>Date</b>
52.215-14	Integrity of Unit Prices	NOV 2021
52.216-7	Allowable Cost and Payment	AUG 2018
52.222-20	Contracts for Materials, Supplies, Articles, and Equipment	JUN 2020
52.230-2	Cost Accounting Standards	JUN 2020
52.230-6	Administration of Cost Accounting Standards	JUN 2010
52.246-26	Reporting Conforming Items	NOV 2021
252.203-7001	Prohibition on Persons Convicted of Fraud or Other Defense-Contract-Related Felonies	DEC 2008
252.203-7004	Display of Hotline Posters	AUG 2019
252.222-7006	Restrictions on the Use of Mandatory Arbitration Agreements	DEC 2010
252.225-7016	Restriction on Acquisition of Ball and Roller Bearings	JUN 2011
252.227-7013	Rights in Technical Data – Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.231-7000	Supplemental Cost Principles	DEC 1991

#### **52.208-8 Required Sources for Helium and Helium Usage Data (AUG 2018)**

##### **(a) Definitions.**

Bureau of Land Management, as used in this clause, means the Department of the Interior, Bureau of Land Management, Amarillo Field Office, Helium Operations, located at 801 South Fillmore Street, Suite 500, Amarillo, TX 79101–3545.

Federal helium supplier means a private helium vendor that has an in-kind crude helium sales contract with the Bureau of Land Management (BLM) and that is on the BLM Amarillo Field Office's Authorized List of Federal Helium Suppliers available via the Internet at <https://www.blm.gov/programs/energy-and-minerals/helium/partners>.

Major helium requirement means an estimated refined helium requirement greater than 200,000 standard cubic feet (scf) (measured at 14.7 pounds per square inch absolute pressure and 70 degrees Fahrenheit temperature) of gaseous helium or 7510 liters of liquid helium delivered to a helium use location per year.

(b) Requirements—(1) Contractors must purchase major helium requirements from Federal helium suppliers, to the extent that supplies are available.

(2) The Contractor shall provide to the Contracting Officer the following data within 10 days after the Contractor or subcontractor receives a delivery of helium from a Federal helium supplier—

(i) The name of the supplier;

(ii) The amount of helium purchased;

(iii) The delivery date(s); and

(iv) The location where the helium was used.

(c) Subcontracts. The Contractor shall insert this clause, including this paragraph (c), in any subcontract or order that involves a major helium requirement.

(End of clause)

### **Prime Contract Clauses – Additional Flowdown Requirements**

#### **C.1.4.1 COST AND SOFTWARE DATA REPORTING (CSDR)**

Cost and Software Data are the primary means by which the Department of Defense (DoD) collects data on the costs that contractors incur on DoD programs. Reliable and comprehensive cost data is essential to produce credible cost estimates as required in both statute and regulation. The Governments goals and use of CSDR data is to improve the quality of cost estimates; ensure proper resource allocation occurs within the DoD; and enable data driven decision making by program and department leadership.

The contractor shall systematically collect, report and deliver IAW Attachment 0108 CSDR Plan actual contract costs IAW the following CDRLs and Attachment 0108 - CSDR Plan:

<u>Report Title</u>	<u>CDRL</u>
Resource Distribution Table	A004
Cost and Hour Report (Flex File)	A005
Quantity Data Report (DD Form 1921-Q)	A006
Technical Data Report (TDR, DD Form 1921-T)	A007
Contractor Business Data Report (DD Form 1921-3)	A008

#### **C.1.4.1.1 APPLICATION TO SUBCONTRACTORS**

This requirements referenced in Section C.1.4.1 shall apply to Seller where the Order value is expected to exceed \$50 million using the maximum allowable contract quantities, hours, or options (as applicable), as required by Department of Defense (DoD) 5000.04-M-1 – CSDR Manual.

The Contractor shall flow-down CSDR requirements referenced in Section C.1.4.1 and its sub-paragraphs to subcontractors (regardless of subcontractor tier) when the subcontract value is expected to exceed \$50 million using the maximum allowable contract quantities, hours, or options (as applicable), as required by Department of Defense (DoD) 5000.04-M-1 - CSDR Manual. The contractor shall require subcontractors to electronically deliver CSDR deliverables directly to the Defense Cost and Resource Center (DCARC). The contractor shall ensure that subcontractors subject to CSDR reporting thresholds collect data in sufficient detail to meet Attachment 0108 – CSDR Plan requirements. The contractor shall collect and deliver data on all subcontractors to comply with Attachment 0108 - CSDR Plan requirements, Attachment 0109 Resource Distribution Table (RDT), and CDRL A004, RDT. A subcontract, per DoDM 5000.04 M-1 Cost and Software Data Reporting Manual, is any agreement, purchase order, or instrument other than a prime contract calling for work or for the material required for the performance of one or more prime contracts. A subcontract usually covers procurement of major components or subsystems that require the subcontractor to do extensive design, development, engineering, and testing to meet a prime contractor's procurement specifications.

#### C.1.4.1.2 RESOURCE DISTRIBUTION TABLE (RDT)

The Contractor shall prepare and deliver the RDT IAW CDRL A004 and Attachment 0109 Resource Distribution Table (RDT). The RDT identifies the value of work assigned to the contractor and its subcontractors for each WBS element listed in Attachment 0108 - CSDR Plan, and is the primary means of identifying subcontractors who qualify for CSDR reporting.

#### C.1.4.1.3 COST AND HOUR REPORT (FLEXFILE)

The contractor shall prepare and deliver the Cost and Hour Report (Flex File) IAW CDRL A005. The Cost and Hour Report (Flex File) reports incurred and forecasted costs and hours related business data in order to perform this contract.

#### C.1.4.1.4 QUANTITY DATA REPORT (DD FORM 1921-Q)

The contractor shall prepare and deliver the Quantity Data Report (DD Form 1921-Q) IAW CDRL A006. The Quantity Data Report (DD Form 1921Q) reports quantity information to deliver context to the data reported in Flex File submissions and in order to derive accurate unit cost information.

#### C.1.4.1.5 TECHNICAL DATA REPORT (TDR, DD FORM 1921-T)

The contractor shall prepare and deliver the Technical Data Report (DD Form 1921-T) IAW CDRL A007. The Technical Data Report (DD Form 1921-T) reports technical parameter data to deliver context to the data reported in Flex File submissions and in order to derive parametric cost estimating relationships.

#### C.1.4.1.6 CONTRACTOR BUSINESS DATA REPORT (CBDR, DD FORM 1921-3)

The contractor shall prepare and deliver the Contractor Business Data Report (DD Form 1921-3) IAW CDRL A008. The Contractor Business

Data Report (DD Form 1921-3) reports data to facilitate estimating and analysis of indirect contract costs and rates.

#### **C.1.4.4.4 APPLICATION TO SUBCONTRACTORS**

The Contractor shall flow down DFARS Clause 252.234-7002 Earned Value Management System. The performance information reported by the Subcontractors shall be incorporated and integrated into the Contractor's management system.

#### **C.1.5.3.4 POST-AWARD SUBCONTRACT CONTENT**

The contractor shall deliver a definitive list of all known or proposed subcontractors and suppliers of critical components with logic bearing components (i.e., software, firmware, network cards, and printed circuit boards) IAW Attachment 0128 - Supplier RFI Form. The list will be reviewed and approved by the Government's Systems Engineer and the Government Security Manager in coordination with Defense Intelligence Agency (DIA). DIA will assess the foreign intelligence and technology exploitation threat for the supply chain associated with the critical components. A threat assessment can take 3-6 months. The results of the threat assessment must be used to inform the subcontractor's risk mitigation strategy for all critical components. Mitigation could include disapproval to use a prospective subcontractor or supplier IAW Sec 806 of NDAA FY 2011 (authority extension in Sec 806 of NDAA FY 2013). The contractor shall take steps to ensure that commercial products purchased or obtained shall not be identified as being destined for inclusion in a Government system IAW CDRL B003, Critical Component Subcontractor and Supplier List.

#### **C.1.6.3 SECURITY REQUIREMENTS**

##### **C.1.6.3.1 SECURITY CLASSIFICATION SPECIFICATION**

The contractor shall adhere to the requirements of Attachment 0104 - JPO JLTV Security Classification Guide (SCG) and Attachment 0102 - Department of Defense Contract Security Classification Specification (DD254), for the protection of the unclassified information, CUI, and Classified information, data, hardware, and software generated for or delivered in support of the program. Classified or unclassified information data not covered under Attachment 0104 - JPO JLTV SCG will follow Attachment 0103 - PEO CS&CSS Armoring Systems SCG. To preserve national security interest, the contractor shall ensure all aspects of the contract and work performed are evaluated for conformance with security procedures and standards. The contractor shall evaluate all products for security implications and prepare appropriate security documents and plans. As needed, the contractor shall participate in discussions on security at quarterly PMRs with the Government.

##### **C.1.6.3.5 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, computer software, 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 CUI and/or U//FOUO information, the contractor shall adhere to the guidelines in Attachment 0104 - JPO JLTV SCG, Attachment 0102 - Department of Defense Contract Security Classification Specification (DD254), DoDM 5200.01 Vol 1- 3, DoDi 5200.48, Army Regulation (AR) 25-55, AR 25-2, AR 380-5, and AR 25-1.

##### **C.1.6.3.6 DISTRIBUTION STATEMENTS**

Marking of Technical Data and Computer Software shall include the statement delivered in Attachment 0104 - JPO JLTV SCG and Attachment 0102 - Department of Defense Contract Security Classification Specification (DD254). If the contents of the technical document require more than one Distribution Statement, apply the most restrictive statement. This does not preclude additional mandated markings



as may be required by the contract. Other requests related to the SCG shall be referred to the Buyer and SFAE-CSS-JL/Security, 6501 E. 11 Mile Road, MS 640, Detroit Arsenal, MI 48397-5000, COM (586) 239-3491.

#### C.1.6.3.7 ENCRYPTION

The contractor shall not transmit any CUI and/or U//FOUO information electronically over the Internet unless it is encrypted by Federal Information Processing Standard (FIPS) 140-3 standard encryption. In order to enable e-mail encryption the contractor shall have or obtain External Certification Authority (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/pki-pke/interoperability/Pages/index.aspx>

#### C.1.6.3.8 OPSEC STANDARD OPERATING PROCEDURE OR PLAN

The contractor shall follow Attachment 0105 - JPO JLTV OPSEC Plan, dated 27 February 2017, as well as annexes and updates. The contractor is not required to develop its own OPSEC Plan. All U.S. contractors shall deliver annual Program specific OPSEC training for all Program personnel. New Program personnel shall receive JPO JLTV OPSEC Plan specific training within 30 calendar days of Program assignment. Annually, contractors shall complete OPSEC training and deliver a report IAW CDRL A012, OPSECT Training Validation Report validating 100% completion to the Government Contracting Office. These requirements, OPSEC Plan and training, shall be flowed down to all U.S. subcontractors with access to CUI and/or classified material.

#### C.1.6.3.9 OPSEC

If the contractor generates unclassified OPSEC sensitive information, this information shall be protected at the same level as U//FOUO and/or CUI information. The contractor 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.1.6.3.9.1 DOD OWNED INSTALLATION OPSEC

Because of antiterrorism/force protection, operations security, and counterintelligence concerns, the contractor shall not release any diagrams, maps, floor plans, schematics, or digital pictures of any DoD owned installations, unless it is necessary for execution of the contract, to outside organizations and companies without the approval of the Contracting Officer and G2 TACOM. All information proposed for public release in any form (video, pictures, article, brochure, web site, etc.) will undergo a Program Executive Office (PEO) Combat Support and Combat Service Support (CS&CSS) OPSEC Review using Attachment 0106 - PEO CS&CSS STA Form 7114.

#### C.1.6.3.10 PROTECTION AND DISCLOSURE OF GOVERNMENT INFORMATION PUBLIC RELEASE REQUESTS

Except for information previously approved for public release by the Government, the Contractor 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 JPO JLTV work at any tier, (iv) Associate Contractors, at any tier, and (v) any other individual or entity that is not contractually bound to protect Information from public release without first obtaining written approval for Public Release. Refer to the Attachment 0104 - JPO JLTV SCG (Page 12, Section 10, OPSEC) on public release of information for additional guidance.

The contractor shall screen all information delivered 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. JPO JLTV information is any Program information on the JLTV effort. Refer to Attachment 0104 - JPO JLTV SCG and Attachment 0102 - Department of Defense Contract Security Classification Specification (DD254) on public release of information for additional guidance. The program requires 45 business days to process the request and render a decision.

The contractor shall deliver 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 Clause 252.204-7000 Disclosure of Information. 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.

During the performance of work on this contract and for any period of time after contract performance, the contractor shall deliver protection to Government Information/Data as required by the DD 254.

#### **C.1.6.3.11 MARKETING PROPOSALS AND EXPORT CONSIDERATIONS**

The contractor shall coordinate with the JPO JLTV office staff and counterintelligence support staff, all proposals to market or otherwise obtain a commercial export license to sell portions of the system being acquired or like systems to foreign countries.

#### **C.1.6.3.12 INFORMATION FLOW DOWN**

The contractor shall ensure the security requirements and guidelines contained in Section C.1.6.3, the program Operations Security

(OPSEC) Requirements (C.1.6.3.11), DD 254 Requirements (Attachment 0102), CUI instruction (C.1.6.3.6), and export control safeguards

(C.1.6.3.13) are contractually flowed down to subcontractors, teammates and consultants.

#### **C.1.6.3.13 THREAT INFORMATION**

The contractor shall evaluate Government-delivered foreign intelligence and technology exploitation threat information, along with the traditional acquisition and battlefield threat information, as part of System Security Engineering (SSE), systems engineering, and procurement decision processes.

#### **C.1.6.3.14 COMPONENT CONTROL**

The contractor shall ensure that products purchased or obtained shall not be identified as being destined for inclusion in a Government system. The contractor shall certify that the underlying software, firmware, and hardware, have been controlled, evaluated, and tested to ensure that the service delivers what it is designed to deliver and nothing more. The contractor shall not deliver functionality, additions, or enhancements to component controls unless explicitly requested and approved in writing by the Government. The contractor shall not knowingly create the capability for unauthorized access to the system or knowingly introduce such capability into the Army network.

#### **C.1.6.3.15 INHERITED CRITICAL PROGRAM INFORMATION AND CRITICAL TECHNOLOGY (CPI/CT)**

Identification of CPI and CT and implementation of AT for inherited technologies is the responsibility of the specific external program(s) that originates the CPI and CT. The contractor shall implement security countermeasures identified by the external program(s) in order to ensure the inherited CPI/CT is protected to the level outlined in the respective inherited technologies program protection plan.

#### **C.2.1.1.1 CONFIGURATION MANAGEMENT (CM)**

The contractor shall execute CM to the JLTV FoV IAW the requirements of this section and all its subsections. The Government shall be the approver of all changes to the configuration baselines and corresponding JLTV FoV TDP and CSP through ECPs IAW CDRL B004 ECP.

Government approval of a change does not constitute relief from vehicle performance requirements unless a formal requirement change to Attachment 0101 - JLTV PD, is delivered and approved by the Government. The contractor shall execute a complete CM program to manage all hardware and software configurations including documentation, electronic media, and parts representing or comprising the JLTV FoV. The contractor shall apply CM functions, including processes, responsibilities, resources, and metrics, throughout the product lifecycle, and flow down these CM requirements to subcontractors to deliver appropriate application of CM function to entire supply chain. The contractor shall make available all of the Contractor's Configuration Management Program documentation including all policies, procedures, and reports to the Government upon request. The Contractor's Configuration Management Plan IAW CDRL B005, CMP shall be IAW SAE EIA-649-1A, Configuration Management Requirements for Defense Contracts. The contractor may also utilize GEIA-859A, Data Management(DM), and DoD MIL-HDBK-61, Configuration Management Guidance.

#### **C.2.1.2.1.3 HAZARD TRACKING LOG (HTL)**

The contractor shall prepare a HTL IAW Task 106 of MIL-STD-882 and the Hazard Tracking Log Content Requirements (Attachment 0118 - Hazard Tracking Log). The Hazard Tracking Log shall document the hazards associated with the system design and the integration of GOTS and GFP items to the system. The contractor shall deliver the HTL IAW CDRL B019, Hazard Tracking Log. The Government will deliver final acceptance on effectiveness of mitigations and the residual risk level. Closed out hazards shall remain on the HTL.

#### **C.2.1.2.4.2 CYBERSECURITY AND SOFTWARE SCANS**

The contractor shall deliver the Government access to the software source code repositories for all JLTV software (excluding closed-source COTS) for Software Code Scans to determine if there are any vulnerabilities in the system. The contractor shall ensure each source code repository can accept the Government's Hewlett Packard (HP) Fortify 360 Suite Static Code Analyzer scanning software tool.

##### **C.2.1.2.4.2.1 BASELINE CYBERSECURITY AND SOFTWARE SCAN**

The contractor shall deliver the Government access to the CSIL for the Baseline Cybersecurity scan. The Baseline Scans shall be held NLT 150 calendar days after Contract Award.

##### **C.2.1.2.4.2.2 FOLLOW-ON CYBERSECURITY SCANS**

The contractor shall deliver the Government access to the CSIL for additional testing identified at the Baseline Cybersecurity and Software Code Scans. The follow-on-scans will only be conducted if the baseline scan requires action on the contractor's part to resolve deficiencies.

##### **C.2.1.2.4.2.3 RECURRING CYBERSECURITY AND SOFTWARE SCANS**

The contractor shall deliver the Government access to the CSIL and software source code repositories for all JLTV software and systems and deliver scans. The scans will be conducted monthly and delivered to

the Government quarterly and following significant changes to the JLTV software or architecture including ECPs with software content. In addition, the Government reserves the right to initiate up to three additional scans per year when Security Controls Assessor validation scans are needed to support maintaining the Authority to Operate (ATO).

Software shall satisfy the requirements of the DISA Application Security and Development Security Technical Implementation Guide (STIG) and other applicable DISA STIGs and minimize the overall Common Weakness Scoring System (CWSS) and Common Vulnerability Scoring System (CVSS) scores of systems on which the software will be installed IAW CDRL B027, Cybersecurity Vulnerability Report.

### C.13 USE OF CLASS I and CLASS II OZONE DEPLETING SUBSTANCES

#### (a) Definitions.

(1) Class I and Class II Ozone-Depleting Substances (CIODS) refers to the class of substances identified in Section 602(a) of the Clean Air Act, (42 U.S.C. 7671a(a)), complete list provided at: <https://www.govinfo.gov/content/pkg/USCODE-2013-title42/html/USCODE-2013-title42-chap85-subchapVI-sec7671a.htm>

(2) Directly requires the use of CIODS means that the Government's specification or technical data package, at any tier, explicitly requires the use of any Class I Ozone-Depleting Substance (CIODS) in performance of the contract.

(3) Indirectly requires the use of CIODS means that the Government's specification or technical data package, while not explicitly requiring the use of any CIODS, does require a feature that the contractor can meet or produce only by the use of CIODS.

(b) Per Section 326 of Public Law 102-484, the Army cannot award any contract that directly or indirectly requires the use of CIODS without the approval of the Senior Acquisition Official, per current Army Policy the approval authority is the Army Acquisition Executive. Thus, no CIODS shall be used in meeting the requirements of this contract. If the use of CIODS is required in the performance of this contract, please notify the Contracting Officer immediately in writing.

(c) No Class II Ozone Depleting Substances shall be required in the performance of this contract without government approval. If the use of Class II ODS is required in the performance of this contract, please notify the Contracting Officer immediately in writing.

### C.14 ACCESS AND GENERAL PROTECTION/SECURITY POLICY AND PROCEDURES

(a) The contractor and all associated subcontractors' employees shall comply with applicable installation, facility, and area commander installation and facility access and local security policies and procedures (provided by the Government representative). 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. The contractor workforce must comply with all personal identity verification requirements (FAR clause 52.204-9 Personal Identity Verification of Contractor 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.

(b) For contractors requiring Common Access Card (CAC). Before CAC issuance, the contractor employee requires, at a minimum, a favorably adjudicated National Agency Check with Inquiries (NACI) or an equivalent or higher investigation in accordance with Army Directive 2014-05, The contractor employee will be issued a CAC only if duties involve one of the following: (1) Both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely; (2) Remote access, via logon, to a DoD network using DoD-approved remote access procedures; or (3) Physical access to multiple DoD facilities or multiple non-DoD federally controlled facilities on behalf of the DoD on a recurring basis for a period of six (6) months or more. At the discretion of the sponsoring activity, an initial CAC may be issued on a favorable review of the FBI fingerprint check and a successfully scheduled NACI at the Office of Personal Management.

(c) For contractors that do not require CAC, but require access to a DoD facility or installation. Contractor and all associated subcontractors employees shall comply with adjudication standards, and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05/AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures elsewhere in Section C; Nondisclosure Statement; for OCONUS locations, refer to the Status of Forces Agreement and other theater regulations.

#### C.19 ARMY INFORMATION SYSTEM (IS) SECURITY REQUIREMENT

CONTRACTOR INVESTIGATION/CLEARANCE. Reference AR25-2, AR 380-67, DoD 5200.2-R and Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12 (31 Jul 2008). All contractors and consultants that access government owned or operated automated information systems, networks, or databases and to safeguard controlled unclassified information shall have a favorable background investigation as required above references positions designated as IT-I, IT-II or IT-III to perform functions stipulated in contract scope of work. The minimum investigative requirements are as follows: ADP-I (AKA: IT-1 or Privileged Access) = Tier 5 (T5) / Tier 5 Reinvestigation (T5R)(AKA: Single Scope Background Investigation (SSBI), Single Scope Periodic Reinvestigation (SSPR) or Phased Period Reinvestigation (PPR)); ADP-II (AKA: IT-2 or Limited Privileged Access) = Tier 3 (T3) / Tier 3 Reinvestigation (T3R)(AKA : Access National Agency Check with Written Inquiries and Credit Check (ANACI) or National Agency Check with Law and Credit Check (NACLC)); or ADP-III (AKA: IT-3 or (Non-Privileged Access) = Tier 1 (T1) / Tier 2 with Subject Interview (T2S) or Tier 2 Reinvestigation with Subject Interview (T2RS) (AKA: National Agency Check with Inquiries (NACI)). A Common Access Card (CAC) may be issued on an interim basis based on favorable T1 or a Federal Bureau of Investigation (FBI) National Criminal History Check (fingerprint check) adjudicated by appropriate approved automated procedures or by a trained security or human resource (HR) specialist, and successful submission to the investigative service provider (ISP) of a T1 investigation or an investigation greater in scope than a T1. Investigations will be coordinated with the G2, TACOM LCMC (AMSTA-CSS / 586-282-6262) and investigations will be through the Personnel Security Investigations Portal Center of Excellence (PSIP COE). Non-U.S. citizens shall be Permanent Resident Aliens with requisite investigation. All personnel shall receive and certify to an Information Systems Security Briefing.

#### **E-6 52.246-11 HIGHER-LEVEL CONTRACT QUALITY REQUIREMENT DEC/2014**

(a) The contractor shall comply with the higher-level quality standard(s) listed below.

Title: IATF 16949:2016 Automotive Quality Management System Standard

Number: IATF 16949

Date: 2016-10-01 (First Edition)

Tailoring: IATF Sanctioned Interpretations (1-11)

(b) The contractor shall include applicable requirements of the higher-level quality standard(s) listed in paragraph (a) of this clause and the requirement to flow down such standards, as applicable, to lower-tier subcontracts in--

(1) Any subcontract for critical and complex items (see 46.203(b) and (c)); or

(2) When the technical requirements of a subcontract require--

(i) Control of such things as design, work operations, in-process control, testing and inspection; or

(ii) Attention to such factors as organization, planning, work instructions, documentation control, and advanced metrology.

(End of clause)

## H.2 ADDITIONAL PROGRAM PROTECTION REQUIREMENTS

The following incidents and situations shall be reported through the Facility Security Officer to the nearest U.S. Army Counterintelligence (CI) office and the Defense Security Service as required by DoD 5220.22-M, National Industrial Security Program Operating Manual. If the U.S. Army CI office is not readily available, the FSO or representative security individual will report the information to the program Government Security Office, which will ensure that reports are relayed, within 24 hours, IAW AR 381-12, Threat and Awareness Reporting Program, to U.S. Army CI:

- a. Attempts by unauthorized persons to obtain classified or unclassified information concerning U.S. Army facilities, activities, personnel, technology, or material through questioning, elicitation, trickery, bribery, threats, coercion, blackmail, photography, observation, collection of documents or material, correspondence, or computer hacking
- b. Known, suspected, or contemplated acts of espionage.
- c. Contacts with persons whom they know or suspect to be members of or associated with foreign intelligence, security, or terrorist organizations. These do not include contacts as a part of official duties.
- d. Contacts with any official or other citizen of a foreign country when that person
  - (1) Exhibits excessive knowledge or undue interest about the employee or his duties
  - (2) Exhibits undue interest in U.S. technology; research, development, testing, and evaluation efforts; weapons systems; or scientific information
  - (3) Attempts to obtain classified or unclassified information
  - (4) Attempts to place employee under obligation through special treatment, favors, gifts, money, or other means
  - (5) Attempts to establish any type of business relationship that is outside the range of normal official duties
- e. All incidents in which employees or their family members traveling to or through foreign countries are
  - (1) Subjected to questions regarding their duties
  - (2) Requested to provide military information
  - (3) Threatened, coerced, or pressured in any way to cooperate with a foreign intelligence service or foreign government official
  - (4) Offered assistance in gaining access to people or locations not routinely afforded Americans.
  - (5) Contacted by foreign government law enforcement, security, or intelligence officials
- f. Information concerning any international or domestic terrorist activity or sabotage that poses an actual or potential threat to Army or other U.S. facilities, activities, personnel, or resources.

- g. Any known or suspected illegal diversion or attempted illegal diversion of U.S. technology to a foreign country.
- h. Active attempts to encourage employees to violate laws, disobey lawful orders or regulations, or disrupt military activities (subversion).
- i. Known or suspected acts of treason.
- j. Participation in activities advocating or teaching the overthrow of the United States by force or violence or seeking to alter the form of Government by unconstitutional means (sedition).
- k. Known, suspected, or attempted intrusions into classified or unclassified information systems by unauthorized users or by authorized users attempting to gain unauthorized access.
- l. Any situation involving coercion, influence, or pressure brought to bear on employees through family members residing in foreign countries.

## **H.5 SPECIAL CONTRACT REQUIREMENT (SCR) FOR IDENTIFICATION AND ASSERTION OF RESTRICTIONS ON TECHNICAL DATA AND COMPUTER SOFTWARE (Intellectual Property)**

Applicability: Seller must abide by this clause where Seller generates or modifies technical data or computer software in connection with any Order.

### **H.5.1 Definitions**

H.5.1.1 Background Patent is defined as any U.S. patent, or U.S. patent application, or PCT patent application, which covers an invention or discovery which is not a subject invention (as defined in FAR 52.227-11) and which is owned or controlled by the Offeror at any time through the completion of this contract or to which the offeror has an interest through inventorship. The specific patent and application numbers and full titles are required to be provided.

H.5.1.2 Terms used in this Special Contract Requirement (SCR) that are defined in the following clauses and SCR have the same meaning as set forth in those clauses and this SCR:

H.5.1.2.1 DFARS 252.227-7013;

H.5.1.2.2 DFARS 252.227-7014;

H.5.1.2.3 DFARS 252.227-7015; or

H.5.1.2.4 DFARS 252.227-7017;

### **H.5.2 Identification and Assertion of Restrictions**

The contractor shall not deliver or otherwise provide to the Government any technical data or computer software with restrictive markings (or otherwise subject to restrictions on access, use, modification, reproduction, release, performance, display, or disclosure) unless the technical data and computer software has been identified in accordance with the following requirements:

#### **H.5.2.2 Pre-Award Identification and Assertions**

In its Assertion of Restrictions (Attachment 0161, Attachment 0172, Attachment 0174) the offeror (including its subcontractors or suppliers, or potential subcontractors or suppliers, at any tier) shall identify all commercial and noncommercial technical data and computer software that is to be delivered or otherwise provided (including all option CLINs as if the option was exercised) including with unlimited rights as follows:

##### **H.5.2.2.1 Noncommercial Technologies**

Offeror shall identify all noncommercial technical data and noncommercial computer software including firmware to be delivered and will provide at least the information as required by DFARS 252.227-7017 (JAN 2011) and IAW Attachment 0161, Attachment 0172, Attachment 0174.

#### H.5.2.2.2 Commercial Technologies

Offeror shall identify all commercial technical data (i.e., technical data pertaining to a commercial item) and commercial computer software including firmware IAW Attachment 0161, Attachment 0172, Attachment 0174.

H.5.2.2.3 The requirements to submit, fully populate and complete, and sign the identification and assertions required by paragraphs H.5.2.2.1 and H.5.2.2.2 of this SCR are considered a material element of source selection and failure to meet this requirement will rendered the offer ineligible for award.

#### H.5.2.3 Post-Award Updates to the Pre-Award Identification and Assertions

Except as provided in this paragraph, the contractor (including its subcontractors or suppliers at any tier) shall not supplement nor revise the pre-award identification and Assertion of Restrictions after contract award.

##### H.5.2.3.1 Noncommercial Technologies

Post-award identification and assertion of restrictions on noncommercial technical data and noncommercial computer software including firmware are governed by paragraph (e) of DFARS 252.227-7013 (FEB 2014) and DFARS 252.227-7014 (FEB 2014), respectively.

##### H.5.2.3.2 Commercial Technologies

The contractor may supplement or revise its pre-award identification and assertion of restrictions commercial technical data and commercial computer software only if such an expansion or revision would be permitted for noncommercial technical data or noncommercial computer software including firmware pursuant to H.5.2.3.1. Approval is contingent upon the PCO determination that changes to assertions would not have materially impacted the source selection.

#### H.5.2.4 Assertion of Restrictions for ECPs

If an ECP will result in the generation of any new data or any changes to the rights proposed at contract award, the contractor shall deliver (with their proposal) a complete Assertion of Restrictions identifying all commercial and noncommercial technical data and computer software that is to be delivered or otherwise provided including with unlimited rights as follows:

##### H.5.2.4.1 Noncommercial Technologies

Contractor shall identify all noncommercial technical data and noncommercial computer software including firmware to be delivered and will provide at least the information as required by DFARS 252.227-7017 (JAN 2011) and IAW Attachment 0161, Attachment 0172, Attachment 0174.

##### H.5.2.4.2 Commercial Technologies

Contractor shall identify all commercial technical data (i.e., technical data pertaining to a commercial item) and commercial computer software including firmware IAW Attachment 0161, Attachment 0172, Attachment 0174.

#### H.5.2.5 Assertion of Restrictions for Work Directives

Throughout the life of the contract for each work directive, with each work directives proposal, the contractor must deliver a complete Assertion of Restrictions. In its Assertion of Restrictions the contractor (including its subcontractors or suppliers, or potential subcontractors or suppliers, at any tier) shall identify all commercial and noncommercial technical data and computer software that is to be delivered or otherwise provided including with unlimited rights as follows:



#### H.5.2.5.1 Noncommercial Technologies

Contractor shall identify all noncommercial technical data and noncommercial computer software including firmware to be delivered and will provide at least the information as required by DFARS 252.227-7017 (JAN 2011) and IAW Attachment 0161, Attachment 0172, Attachment 0174.

#### H.5.2.5.2 Commercial Technologies

Contractor shall identify all commercial technical data (i.e., technical data pertaining to a commercial item) and commercial computer software including firmware IAW Attachment 0161, Attachment 0172, Attachment 0174.

#### H.5.3 Copies of Negotiated, Commercial, and Other Non-Standard Licenses

H.5.3.1 Contractor shall provide copies of all proposed specially negotiated licenses(s), commercial license(s) including open source software licenses, and any other asserted restrictions other than unlimited rights; Government purpose rights; limited rights; restricted rights; STTR data rights; SBIR data rights for which the protection period has not expired; or Government's minimum rights as specified in the clause at DFARS 252.227-7015.

H.5.3.2 In the event the offeror or contractor proposes specially negotiated license rights, it shall include the content and be in the format provided in Attachment 0180 - Specifically Negotiated License Agreement TDP and CSP Purchase Option, for the Technical Data, Computer Software and Patent License Identification and Assertions Listed in Attachment 0161, Attachment 0172, or Attachment 0174, unless a similar content and format is approved, in writing, by the PCO prior to proposal submission.

H.5.4 In the event the Contractor asserts rights to technical data or computer software, the Contractor shall fully abide by H.5.

H.5.5 In the event the offeror asserts rights to technical data or computer software, the offeror shall fully abide by H.5.

H.5.6 In the event a subcontractor generates or modifies technical data or computer software, the Contractor shall flow-down H.5 to that subcontractor.

36388547.1