XM30 Program (W56HZV-23-C-0026) FlowDown FAR/DFARS Clauses for all Subcontractors

Clause # (Link)	Description	Included in XM30 Contract	Section(s) XM30 Contract	Mandatory FlowThrough (Y/N) XM30 Contract	Comments
252.203-7000	REQUIREMENTS RELATING TO COMPENSATIN OF FORMER DOD OFFICIALS	Yes	I	Yes	
252.203-7001	PROHIBITION ON PERSONS CONVICTED OF FRAUD OR OTHER DEFENSE - CONTRACT-RELATED FELONIES	Yes	I	Yes	
252.203-7002	REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	Yes	I	Yes	
252.203.7004	DISPLAY OF HOTLINE POSTERS	Yes	I	Yes	
252.204-7000	Disclosure of Information	Yes	I	Yes	
252.204-7009	Limitation on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	Yes	I	Yes	*The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.
252.204-7012	Safeguarding Covered Defense Information and Cyber Incident Reporting	Yes	I	Yes	
252.204-7015	Notice of Authorized Disclosure of Informationfor Litigation Support	Yes	I	Yes	
252.204-7018	Prohibition on the acquisition of covered defense telecommunications equipment or services	Yes	I	Yes	
252.204-7020	NIST SP 800-171 DOD Assessment Requirements	Yes	I	Yes	
252.211-7003	ITEM UNIQUE IDENTIFICATION AND VALUATION	Yes	I	Yes	
252.222-7006	Restrictions on the Use of Mandatory ArbitrationAgreements	Yes	I	Yes	
252.223.7002	SAFETY PRECAUTIONS FOR AMMUNITION AND EXPLOSIVES	Yes	I	Yes	* To be flowed down in every subcontract that involves ammunition or explosives.
252.223-7006	Prohibition on storage, treatment, and disposal of toxic and Hazardous Materials - Basic	Yes	I	Yes	
252.223-7007	SAFEGUARDING SENSITIVE CONVENTIONAL ARMS, AMMUNITION, AND EXPLOSIVES	Yes	I	Yes	* To be flowed down in every subcontract (1) For the development, production, manufacture, or purchase of AA&E; or (2) When AA&E will be provided to the subcontractor as Government-furnished property.
252.223-7008	PROHIBITION OF HEXAVALENT CHROMIUM	Yes	I	Yes	
252.225-7007	Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies (DEC 2018)	Yes	I	Yes	
252.225-7009	RESTRICTION ON ACQUISITION OF CERTAIN ARTICLES CONTAINING SPECIALTY METALS	Yes	I	Yes	*The Contractor shall exclude and reserve paragraph (d) and this paragraph (e)(1) when flowing down this clause to subcontracts.
252.225-7012	Preference for Certain Domestic Commodities	Yes	I	Yes	
252.225-7013	Duty Free Entry (Deviation 2020-O0019)	Yes	I	Yes	
252.225-7016	RESTRICTION ON ACQUISITION OF BALL AND ROLLER BEARINGS	Yes	I	Yes	
252.225-7033	WAIVER OF UNITED KINGDOM LEVIES	Yes	I	Yes	
252.225-7048	Export-Controlled Items	Yes	I	Yes	
252.225-7052	Restriction on the Acquisition of Certain Magnets, Tantalum, and Tungsten	Yes	I	Yes	
252.225-7056	PROHIBITION REGARDING BUSINESS OPERATION WITH THE MADURO REGIME	Yes	I	Yes	
252.225-7972	PROHIBITION ON THE PROCUREMENT OF FOREIGN-MADE UNMANNED AIRCRAFT SYSTEMS (DEVIATION 2020-O0015)	Yes	I	Yes	*Clause does not exist yet on acquisition.gov. However, was able to locate it on farclause.com. Add to list to be submitted to the USG (ARV is questioning if this clause is applicable).
252.227-7013	Rights in Technical Data --Noncommercial Items	Yes	I	Yes	
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	Yes	I	Yes	

Clause # (Link)	Description	Included in XM30 Contract	Section(s) XM30 Contract	Mandatory FlowThrough (Y/N) XM30 Contract	Comments
252.227-7015	Technical Data --Commercial Items	Yes	I	Yes	
252.227-7016	Rights in Bid or Proposal Information	Yes	I	Yes	
252.227-7019	Validation of Asserted Restrictions - Coputer Software	Yes	I	Yes	
252.227-7037	Validation of Restrictive Markings on Technical Data	Yes	I	Yes	
252.227-7038	Patent Rights - Ownership by the Contrctor (Large Business)	Yes	I	Yes	
252.227-7038	PATENTS -- OWNERSHIP BY THE CONTRACTOR (LARGE BUSINESS) (JUN 2012) -- DEC/2007 ALTERNATE I (DEC 2007)	Yes	I	Yes	
252.242-7005	Contractor Business Systems	Yes	I	Yes	
252.244-7000	Subcontracts for Commercial Items	Yes	I	Yes	
252.246-7001	Warranty of Data (Mar 2014) - Alternate II (Mar 2014)	Yes	I	Yes	
252.246-7007	CONTRACTOR COUNTERFEIT ELECTRONIC PART DETECTION AND AVOIDANCE SYSTEM	Yes	I	Yes	Does not apply unless the Contractor is subject to the Cost Accounting Standards under 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201-1.
252.246-7008	SOURCES OF ELECTRONIC PARTS	Yes	I	Yes	
252.247-7023	Transportation of Supplies by Sea -- Basic	Yes	I	Yes	
252.249-7002	Notification of Anticipated Contract Termination or Reduction	Yes	I	Yes	
52.203-12	Limitation on Payments to Influence Certain Federal Transactions.	Yes	I	Yes	
52.203-13	Contractor Code of Business Ethics and Conduct.	Yes	I	Yes	
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements.	Yes	I	Yes	
52.203-6	Restrictions on Subcontractor Sales to the Government.	Yes	I	Yes	
52.203-7	Anti-Kickback Procedures.	Yes	I	Yes	
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards.	Yes	I	Yes	
52.204-2	Security Requirements.	Yes	I	Yes	
52.204-21	Basic Safeguarding of Covered Contractor Information Systems.	Yes	I	Yes	
52.204-23	Prohibition on Contracting for Hardware Software and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.	Yes	I	Yes	
52.204-25	Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.	Yes	I	Yes	
52.204-27	Prohibition on a ByteDance Covered Application (2023)	Yes	I	Yes	This clause was added per Contract Modification P00001. *The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.
52.204-9	Personal Identity Verification of Contractor Personnel.	Yes	I	Yes	
52.209-6	Protecting the Government?ÇÖs Interest When Subcontracting with Contractors Debarred Suspended or Proposed for Debarment.	Yes	I	Yes	
52.211-15	Defense Priority and Allocation Requirements.	Yes	I	Yes	
52.215-14	Integrity of Unit Prices.	Yes	I	Yes	
52.215-15	Pension Adjustments and Asset Reversions.	Yes	I	Yes	
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions.	Yes	I	Yes	

Clause # (Link)	Description	Included in XM30 Contract	Section(s) XM30 Contract	Mandatory FlowThrough (Y/N) XM30 Contract	Comments
52.215-2	AUDIT AND RECORDS--NEGOTIATIONS	Yes	I	Yes	*If this is a cost-reimbursement, incentive, time-and-materials, labor-hour, or price redeterminable contract, or any combination of these, the Contractor shall maintain and the Contracting Officer, or an authorized representative of the Contracting Officer, shall have the right to examine and audit all records and other evidence sufficient to reflect properly all costs claimed to have been incurred or anticipated to be incurred directly or indirectly in performance of this contract.
52.219-4	Notice of Price Evaluation Preference for Hubzone Small Business Concerns	Yes	I	Yes	
52.219-9	Small Business Subcontracting Plan.	Yes	H & I	Yes	
52.222-21	Prohibition of Segregated Facilities.	Yes	I	Yes	
52.222-26	Equal Opportunity.	Yes	I	Yes	
52.222-35	Equal Opportunity for Veterans.	Yes	I	Yes	
52.222-36	Equal Opportunity for Workers with Disabilities.	Yes	I	Yes	
52.222-37	Employment Reports on Veterans.	Yes	I	Yes	
52.222-40	Notification of Employee Rights Under the National Labor Relations Act.	Yes	I	Yes	
52.222-50	Combating Trafficking in Persons.	Yes	I	Yes	
52.222-54	Employment Eligibility Verification.	Yes	I	Yes	
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving.	Yes	I	Yes	
52.225-13	Restrictions on Certain Foreign Purchases.	Yes	I	Yes	
52.227-1	Authorization and Consent.	Yes	I	Yes	
52.227-10	Filing of Patent Applications-Classified Subject Matter.	Yes	I	Yes	
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement.	Yes	I	Yes	
52.228-5	INSURANCE--WORK ON A GOVERNMENT INSTALLATION	Yes	I	Yes	*The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation
52.232-40	Providing Accelerated Payments to Small Business Subcontractors.	Yes	I	Yes	
52.234-1	Industrial Resources Developed Under Title III Defense Production Act.	Yes	I	Yes	
52.244-6	Subcontracts for Commercial Items.	Yes	I	Yes	
52.245-1	GOVERNMENT PROPERTY	Yes	I	Yes	
52.247-63	Preference for U.S.-Flag Air Carriers.	Yes	I	Yes	
52.247-68	REPORT OF SHIPMENT (REPSHIP)	Yes	I	Yes	

SECTIONS H Special Contract Requirements INCORPORATED IN FULL TEXT:	
Para	**Description**
H.1	**Special Contract Requirement (SCR) for Identification and Assertion of Restrictions on Technical Data and Computer Software (Intellectual Property)**
H.1.1	**Definitions.**
H.1.1.1	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.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.1.2.1	DFARS 252.227-7013;
H.1.2.2	DFARS 252.227-7014;
H.1.2.3	DFARS 252.227-7015;
H.1.2.4	DFARS 252.227-7017;

H.1.2.5	Attachment 0013 (Special License Requirements) for Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions); or
H.1.2.6	Delivery and License Rights for Technical Data and Computer Software Necessary for Operation, Maintenance, Installation, and Training (OMIT), Section H.9.
H.1.3	**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 or computer software has been identified in accordance with the following requirements:
H.1.3.1	**Pre-Award Identification and Assertion**
	In Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions) 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 it proposed to be delivered or otherwise provided including with unlimited rights.:
H.1.3.1.1	**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 DFARS 252.227-7017 (JAN 2011) and IAW Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions).
H.1.3.1.2	**Commercial Technologies**
	Offeror shall identify all commercial technical data (for example technical data pertaining to a commercia item) and commercial computer software including firmware IAW Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions).
H.1.3.1.3	Offeror shall identify whether the technical data or computer software pertains to a modular system interface.
H.1.3.1.4	The requirements to submit, fully populate and complete, and sign the identification and assertions required by paragraphs H.1.3.1.1 to H.1.3.1.3 of this SCR are considered a material element of source selection and failure to meet this requirement may render the offer ineligible for award.
H.1.3.2	**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 Assertions (Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions)) after contract award.
H.1.3.2.1	The Government requests the intellectual property rights for the OMFV to: (1) Reduce the cost and increase the speed of future incremental upgrades, (2) Reduce sustainment costs, (3) Enable organic maintenance, (4) Allow the government to use advance manufacturing and other innovative techniques to reduce the time for vehicle repairs, (5) Support Foreign Military Sales (FMS), and (6) Use OMFV technical data or software on other government programs.
H.1.3.2.2	**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.1.3.2.3	**Commercial Technologies.**
	The Contractor may supplement or revise its pre-award identification and assertion of restrictions in commercial technical data and commercial computer software, including firmware, only if such an expansion or revision would be permitted for noncommercial technical data or noncommercial computer software including firmware pursuant to paragraph H.1.3.2.2 of this SCR (for example based on new information, or inadvertent omissions that would not have materially affected source selection).
H.1.3.2.4	When requested by the Contracting Officer, the Contractor shall provide sufficient information to enable the Contracting Officer to evaluate the Contractor's assertions. The Contracting Officer reserves the right to add the Contractor's assertions to the Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions) and except for commercial computer software, validate any listed assertion at a later date in accordance with the procedures of the Validation of Restrictive Markings on Technical Data and computer software clauses of this contract.
H.1.3.2.5	Contractor shall identify whether the technical data or computer software pertains to a modular system interface.

H.1.4	**Specific Identification of Technical Data and Computer Software**
	When identifying and asserting restrictions on technical data and computer software pursuant to H.1.3.1 and H.1.3.2 of this SCR, the Contractor shall-
H.1.4.1	Ensure that the technical data and computer software are identified by specific reference to the requirement to deliver or provide that technical data or computer software in the contract, for example, by referencing the associated CDRLs.
H.1.4.2	Regarding any computer software that is re-hosted, modified, or developed exclusively or partially at Government expense, the asserted restrictions on the associated data license rights shall specifically address source code, object code, executable code, documentation, software support tools, Software/Systems Engineering Environment documentation, Systems/Software Requirement Documents, Interface Control Documents, etc.
H.1.4.3	Include any relevant information for all technical data and computer software that are or may be required to be delivered or otherwise provided under the contract including online or remote access to information, and firmware or other computer software to be embedded in hardware deliverables.
H.1.5	**Copies of Negotiated, Commercial, and Other Non-Standard Licenses**
H.1.5.1	Contractor shall provide copies of all existing and 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.1.5.2	In the event the Contractor proposes specially negotiated license rights, it shall include the content and be in the format provided in Attachment 0013 (Special License Requirements) for the Technical Data, Computer Software and Patent License Identification and Assertions Listed in Attachment 0012 (Technical Data, Computer Software and Patent License Identification and Assertions) unless a similar content and format is approved, in writing, by the PCO prior to proposal submission.
H.2	**Organizational Conflicts of Interest (OCI)**
H.2.1	The Contractor and its subContractors, consultants, parent companies, subsidiaries, joint ventures (JVs), or other business affiliates, at any tier, may be excluded from performing under this MCS-OMFV contract, if the PCO determines that an OCI exists due to bias or unfair competitive advantage.
H.2.2	The Contractor shall flow down this provision in any subcontracts or other related instruments. The Contractor shall monitor its activities and the activities of its subContractors and related entities, and promptly disclose any actual or potential OCIs and any actions taken or proposed to negate or mitigate such conflicts.
H.2.3	Remedies. For breach of any of the above restrictions or for nondisclosure or misrepresentation of any relevant facts required to be disclosed concerning this contract, the Government may terminate the contract for default, disqualify the Contractor for subsequent related contractual efforts, and pursue such other remedies as may be permitted by law or this contract.
H.3	**Definition(s)**
H.3.1	"Days" As referred to in this contract, the number of days refers to calendar days unless stated otherwise.
H.3.2	"Government-Off-The-Shelf (GOTS)" A software and/or hardware product that is developed by the technical staff of a Government organization for use by the U.S. Government, or developed by an external entity, with specification from the Government organization to meet a specific Government purpose, and can normally be shared among Federal agencies without additional cost. GOTS products and systems are not commercially available to the general public. Sales and distribution of GOTS products and systems are controlled by the Government.
H.4	**Governments Use of Source Selection Cost/Price Proposal Information**
H.4.1	The Government has the right to duplicate and use the awarded Contractor's cost/price proposal information it submitted in response to Solicitation W56HZV-22-R-0026 for the purposes of administering and modifying this contract.
H.5	**Utilization of Small Business Concerns and Subcontracting Plan Compliance Surveillance**

H.5.1	Achievement of Utilization of Small Business Concerns (applies to all Contractors). The Contractor will be required, upon request by the Contracting Officer to provide rationale and/or evidence to substantiate its compliance with the Utilization of Small Business Concerns clause (FAR 52.219-8) as part of the monitoring throughout contract performance. The Contracting Officer will request such information at a minimum of twice a year (for other-than-small businesses, in conjunction with the eSRS reporting periods outlined in FAR 52.219-9 (Alt II)), to assess the Contractor's performance of this requirement.
H.5.2	Achievement of Subcontracting Goals in the Small Business Subcontracting Plan (Not applicable to US Small Business Concerns). The Contractor's performance against subcontracting goals in the Small Business Subcontracting Plan incorporated in this contract will be monitored IAW FAR Clause 52.219-9 (Alt II) by the Contracting Officer for the duration of the contract. The Contractor shall, upon request by the Contracting Officer, provide rationale and/or evidence to substantiate its good faith effort to comply with its subcontracting goals as part of the monitoring throughout contract performance. The rationale and/or evidence that the Contractor is requested to provide may be in addition to the explanations relating to the use of small businesses and the attainment of subcontracting goals that the Contractor has entered in the "Remarks" section of its eSRS submission(s). The Contractor's efforts towards small business utilization on this contract will be included and evaluated as part of Contractor Performance Assessment Reporting System (CPARS). FAR 52.219-9(k)(2) states that a failure of the Contractor or subContractor to comply in good faith with the subcontracting plan incorporated into this contract is considered a breach of contract. The Government will invoke liquidated damages if the Contracting Officer makes a determination that the Contractor has failed to make a good faith effort to comply with the requirements of the subcontracting plan incorporated in this contract, as prescribed in FAR Clause 52.219-16, Liquidated Damages -- Subcontracting Plan.
H.5.3	The Contractor's Subcontracting Plan, dated [to be determined at contract award], is incorporated into the contract (Attachment [to be determined at contract award]).
H.6	**Restrictions on Use**
H.6.1	The Contractor shall identify all the restrictions on the U.S. Government's international use, transportation, use, modification, reproduction, release, perform, display, or disclosure of the Contractor's (or subs, or vendors) technology, hardware, computer software, etc. This includes use and transportation of the technology, hardware, computer software in whole or in part outside the U.S. This includes any restrictions on the use or transportation based on laws, regulations, etc. of any country, in particular but not limited to export/trade control laws and regulations, end use/user certificates, etc. This is to include use or transportation of the technology, hardware, computer software, etc. either as an embedded element of the vehicle or vehicle system, or as a stand-alone part/system as in the case of
H.7	**Security Guidelines**
H.7.1.	**Security Classification Specification**
	The Contractor shall adhere to requirements IAW Attachment 0072 (DD Form 254, Contract Security Classification Specification) for the protection of the unclassified information, CUI, and classified information, data, hardware, and software generated for or provided in support of the program. 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 as identified in this contract, the NISPOM rule and the DD Form 254.
H.7.2	**Classification**
	The highest classification associated with this contract is Secret. The Contractor shall ensure personnel needing access to classified information meet clearance and access requirements. Refer to the DD Form 254 for additional security and personnel requirements.
H.7.3	**Manage Security**
	The Contractor shall manage security activities at the unclassified, CUI, and all applicable classification levels encompassing all security disciplines (Information Security, Operations Security, Anti-Terrorism and Force Protection, International Security, Physical Security, Communications Security, Information Systems Security, and Personnel Security). This requirement is to utilize the above security functions to protect the programs information and technology.
H.7.4	**Controlled Unclassified Information (CUI)**
	CUI provided to or generated pursuant to this contract shall be protected. The procedures for the protection of CUI are outlined in the CUI Attachment to the DD Form 254 and DFARS 252.204-7012. The Contractor shall ensure any covered defense information provided by the

	Government under this contract is destroyed or sanitized from Contractor-owned media and reported in accordance with NIST Special Publication (SP) 800-88, Rev 1, Guidelines for Media Sanitization, December 2014, or returned to the owning organization upon the completion of the contract or as directed by the Contracting Officer.
H.7.5	**Public Release Requests**
	The Contractor shall screen all information submitted for determination of public release to ensure it is both unclassified and technically accurate. The Contractor shall provide a letter of transmittal certifying a screening was conducted and that the Contractor attests that the information is unclassified and technically accurate, to the best of the Contractor's knowledge. The Contractor shall not release program information outside of program channels until the Government review process is complete. The Contractor shall submit all requests for public release approval through the Procuring Contracting Officer (PCO) for a review by Government technical and security personnel and by the Government's Public Affairs Officer (PAO). The PCO 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. The program requires 45 calendar days to process the request and render a decision. 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 a Compact Disc/Digital Video Disc (CD/DVD) using U.S. Postal First Class mail.
H.7.6	**TEMPEST Requirements**
	Prior to the implementation of any TEMPEST countermeasures or expenditure of funds, a TEMPEST assessment will be conducted at every Contractor facility electronically processing classified information. TEMPEST assessments will be marked at a minimum of CUI or classify according to content. The Army TEMPEST staff will review the information provided and determine if a formal TEMPEST Countermeasures Review (TCR) is required. Notification will be provided by the Government Security Manager to the point of contact identified in the submission. The Contractor will send in a TCR request for their facility within 30 days after contract award to the MCS Security Manager, Daniel Kennard (daniel.k.kennard3.civ@mail.mil). The TCR request, if unclassified, shall be sent electronically via encrypted email using cryptographic products that are National Standards and Technology/National Information Assurance Partnership (NIST/NIAP) approved or mail using U.S. Postal First Class mail. If the TCR request is classified, please contact the MCS Security Manager, Daniel Kennard for instruction. This requirement shall be flowed down to all U.S. subContractors that use Information Systems to process classified material. This meets the requirements as identified in the DFARS 252.239-7000 and AR 380-27.
H.7.7	Common Access Card (CAC) or Installation Access Identification: Issuance of a CAC is authorized to U.S. Citizens under this contract if one of the following requirements under Issuance is met.
H.7.7.1	Issuance: The Contractor employee shall be issued a CAC only if duties involve one of the following: (1) Logical access to a DoD network that requires a CAC for login or a DoD website that only accepts the CAC for login access; or (2) Both physical access to a DoD facility and access, via logon, to DoD network on-site or remotely. Access to a DoD network must require the use of a computer with Government-controlled configuration or use of a DoD-approved remote access procedure in accordance with Defense Information Systems Agency; 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 6 months or more. Contractor employees who meet these requirements shall be issued a CAC as explained at http://www.cac.mil/common-access-card/getting-your-cac/for-Contractors/ . Contractor employees who do not meet the requirements for a CAC but are required to have access to a government installation shall be sponsored for an installation Identification card by the contracting officers representative (COR) and provide all information to 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 agreements and other theater regulations.

H.7.7.2	Protection and Handling of Identification (ID) Cards and Reporting Lost or Stolen Cards: For CAC, refer to http://www.cac.mil/common-access-card/managing-your-cac/ . Installation identification or badge shall be displayed while on the installation on the front of the outer garment between the shoulder and waist. The Contractor is responsible for ensuring all ID cards are properly safeguarded and accounted for at all times. The Contractor shall immediately file an installation police report in cases of loss, theft, forgery, or damage and report to the COR.
H.7.7.3	Return of ID Cards: The Contractor shall ensure that all employees, including all subContractor employees at all tiers, return installation and/or access badges in accordance with (IAW) FAR 52.204-9 to the Visitor Control Center for deactivation and destruction. If a Contractor employees badge is not returned, the Contractor shall report, as soon as the incident is discovered, the unrecovered badge to the Installation Police. Contractor employees in possession of a CAC shall be responsible for turning in the CAC IAW FAR 52.204-9 and providing the CAC to the COR. All ID cards (installation or CAC) are property of the U.S. Government.
H.7.8	**Access to Government Information Systems Requirements**
	All Contractor employees with access to a government info system shall be registered in the ATCTS (Army Training Certification Tracking System) https://atc.us.army.mil/iastar/index.php . All Contract employees shall complete the DOD Information Assurance Awareness training prior to be granted access to the government information systems. This training is required to be completed annually for the duration of the contract. The minimum security investigative requirements for access to government information systems is Tier 1 formally known as National Agency Check with Inquiries (NACI) and DISS needs to reflect IT-III (Non-Privileged Access).
H.7.9	**Information Flow Down**
	The Contractor shall ensure the security requirements and guidelines contained in section H.7 and C.9.5 is flowed down to U.S. SubContractors and consultants.
H.7.10	**Compliance to NIST SP 800-171**
H.7.10.1	Release of Controlled Unclassified Information shall only be made to companies who have a valid of a NIST 800-171 basic assessment IAW DFARS 252.204-7020.
H.7.10.2	The Contractor shall submit to NIST 800-171 Medium assessments IAW DFARS 252.204-7020
H.7.10.3	The Contractor shall identify in their SSP and POAM their plans to implement the NIST SP 800-171 Requirements IAW DFARS 252.204-7019 and DFARS 252.204-7020, and will also include the following requirements:
H.7.10.3.1	Implement Requirement 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, a combination of physical and logical protections acceptable to the Government may be substituted;
H.7.10.3.2	Implement Requirement 3.1.5 (least privilege) and associated Requirements, and identify practices that the Contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its SubContractors, suppliers, or vendors based on need-to-know principles;
H.7.10.3.3	Implement Requirement 3.1.12 (monitoring and control remote access sessions)-Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods;
H.7.10.3.4	Audit user privileges on at least an annual basis;
H.7.10.3.5	Implement Requirement 3.13.11 (Federal Information Processing Standards (FIPS) 140-2 validated cryptology or implementation of National Security Agency- or NIST-approved algorithms (i.e., FIPS 140-2 Annex A: Advanced Encryption Standard (AES) Or Triple Data Encryption Standard (DES) or compensating controls as documented in a SSP and POAM));
H.7.10.3.6	Implement Requirement 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which can be evaluated by the Government Program Manager for risk to the program;
H.7.10.3.7	Implement Requirement 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.
H.8	**Prototype Option**
H.8.1	The Government has a unilaterally right to exercise an option up to 4 prototype vehicles (CLIN 0003). The price of 4 prototype vehicles is $.

H.8.2	The prototype option (CLIN 0003) may be exercised unilaterally by the Government at any time, but not later than 31 December 2024. The Government reserves the right to exercise the option in more than one increment for any quantity up to 4 cumulative total prototypes at any time until 31 December 2024 at the pro rata price of the quantity exercised to the total option price. The funding schedule at B.1.2 will be adjusted to show the funding for the option quantity awarded and any remaining quantity. The Government also has the right to specify which prototype(s) (Option Prototype 1-4) are exercised. Deliveries will follow the previously awarded vehicles continuing at the rate of 2 prototypes per month regardless of that shown in Attachment 0051 (PPT Schedule), which will be modified to reflect the option exercise.
H.8.3	If exercised, Attachment 0044 (GFP List) will be modified to incorporate the same GFP for the option prototypes as those previously awarded.
H.9	Delivery and License Rights for Technical Data and Computer Software Necessary for OMIT
H.9.1	Definitions
H.9.1.1	Installation means infrastructure such as facility planning, site surveys, maintenance facilities, supply chain management, test cells, test stands and benches, tools, support equipment, communications, data links, security, data information technology, and all other data and planning used in the initial standup and continued operations, training, sustainment, and maintenance at all operational sites as well as Field Level Maintenance (as defined below in H.9.1.5) and Depot Level Maintenance (as defined below in H.9.1.4) requirements in support of the OMFV.
H.9.1.2	Operation means all procedures, guidance, and instructions for operating, testing, utilization of, familiarization of, emergency use of, and functional use of the OMFV to perform its intended functions. Operation also includes identifying, cataloging, stocking, sourcing, acquiring, procuring, replenishing, packaging, handling, storing, and transporting any OMFV.
H.9.1.3	Maintenance means all activities to maintain, sustain, inspect, test, service, adjust, troubleshoot, analyze, remove, replace, repair, install, disassemble, reassemble, or overhaul (to maintain in, or restore to, an OMFV to a serviceable condition) and to update any changes to the required data. Maintenance includes Depot Level Maintenance (as defined below in H.9.1.4) and Field Level Maintenance (as defined below in H.9.1.5).
H.9.1.4	Depot Level Maintenance as used in this contract includes:
H.9.1.4.1	installation, inspection, localization, isolation, disassembly, interchange, repair, reassembly, alignment, checkout;
H.9.1.4.2	maintenance performed, including modification, testing and reclamation, on material requiring repair, major overhaul, or complete rebuild of parts, assemblies, subassemblies, and end items.
H.9.1.4.3	computer software maintenance (as defined below in H.9.1.6);
H.9.1.4.4	Prognostic and Predictive Maintenance (C.7.4);
H.9.1.4.5	maintenance performed for continuous mission performance.
H.9.1.4.6	Depot Level Maintenance does not include the manufacture of new items but may include the overhaul or refurbishment or remanufacture of existing items.
H.9.1.5	Field Level Maintenance is on-platform maintenance exclusively performed in the field. Field Level Maintenance includes: inspection, service, lubrication, adjustment, calibration, preventive maintenance, repair, replacement, as well as the replacement of parts, minor assemblies, and subassemblies. Field Level Maintenance includes Prognostic and Predictive Maintenance.
H.9.1.6	Computer Software Maintenance as used in this contract includes the repair of code to accomplish its original purpose, regardless of whether or not the maintenance results in a new software release version. Software Maintenance, however, does not include enhancement of the source code capability.
H.9.1.7	Training means formal and informal classroom, training aids, devices, simulations and simulators (TADSS), embedded training, supervised and unsupervised instruction in the operation, use, testing, supply chain management, or maintenance of the OMFV.
H.9.1.8	Required OMIT Data includes all technical data, including development tools (including compilers); computer software (including source code and scripts and libraries used by the source code); computer software documentation; computer databases and graphics pertaining to the OMFV that is required or used when conducting OMIT activities, regardless of whether such activities are performed by military, civilian, or third party contract personnel.
H.9.1.9	Terms used in this SCR that are defined in the following clauses and SCR have the same meaning as set forth in those clauses and this SCR:
H.9.1.9.1	DFARS 252.227-7013;

H.9.1.9.2	DFARS 252.227-7014;
H.9.1.9.3	DFARS 252.227-7015; and
H.9.1.9.4	Attachment 0013 (Special License Requirements).
H.9.2	**License Rights in Required OMIT Data**
H.9.2.1	In accordance with DFARS clause 252.227-7013(b)(1)(v), the Government is granted unlimited rights in technical data that are necessary for installation, operation, maintenance, and training purposes (other than detailed manufacturing or process data). Similarly, in accordance with DFARS clause 252.227-7015(b)(1)(iv), the Government is granted the unrestricted right to use, modify, reproduce, release, perform, display, or disclose technical data, and to permit others to do so, that \'85 (iv) [a]re necessary for operation, maintenance, installation, or training (other than detailed manufacturing or process data). Pursuant to DFARS clause 252.227- 7014(b)(1)(ii), the Government is granted unlimited rights in non-commercial [c]omputer software documentation required to be delivered under this contract.
H.9.2.2	Required OMIT Data that is commercial computer software shall be delivered to the Government subject to a commercial license..
H.9.3	**Delivery of Required OMIT Data**
H.9.3.1	Pursuant to CLIN 0004, the Contractor shall deliver all Required OMIT Data. For all Required OMIT Data, the Contractor shall deliver a complete package of all technical data and computer software for enabling the Government (or third party contract personnel) to perform maintenance of the OMFV without exception. This includes technical data and computer software used in the installation and de- installation, and disassembly and reassembly, at the lowest practicable segregable level. Examples of Required OMIT Data that the Government needs to perform Maintenance includes, but is not limited to, the following:
H.9.3.1.1	Detailed technical data and information regarding all systems;
H.9.3.1.2	Depot Level and Field Level Maintenance technical data (as defined above) and required data regarding all systems, subsystems, and components;
H.9.3.1.3	Interface Control Documents (ICDs);
H.9.3.1.4	Computer software source code necessary to perform maintenance of computer programs and scripts;
H.9.3.1.5	Computer software libraries used by source code necessary to perform maintenance of computer programs and scripts;
H.9.3.1.6	Computer software compilers and computer software tools necessary to perform maintenance of computer programs and scripts; and
H.9.3.1.7	Computer software and computer software documentation necessary to perform maintenance on computer programs and scripts.
H.9.3.1.8	For purposes of this contract, Required OMIT Data includes:
	a. Logistics analysis and related data b. Prognostics and Predictive Maintenance data and software c. Diagnostics data and software d. Provisioning data e. Packaging data f. Technical Publications data g. FIK and Tools data h. Training data i. Embedded Training data and software j. States and Modes of Operation k. System and sub-system faults l. Raw sensor data m. External communications data n. Vehicle and system control signals
	H.9.3.2 Required OMIT Data of SubContractors and Suppliers. The Contractor's obligations set forth in this special contract requirement, H.9, shall apply regardless of whether the Required OMIT Data is (was) developed, delivered, or otherwise provided by its subContractors or suppliers at any tier, and regardless of the items commerciality. Therefore, the Contractor shall flow down the requirements set forth in this special contract requirement, H.9, and shall include these requriements in its subcontracts or other contractual or legal instruments with its subContractors or suppliers at any tier.

H.10	**Technical data and computer software proprietary markings**
	Technical data and computer software that is delivered with unlimited rights must not contain proprietary markings.
H.11	**Development funding for items, components, processes, and computer software**
	For all items, components, processes, or computer software where development is required under this contract, the Contractor shall not absorb or self fund all or any portion of the costs associated with such development without prior written approval of the PCO. Unless otherwise authorized by the PCO, all items, components, processes and computer software developed under this contract shall be developed with direct Government funding including those items components, processes and computer software developed by subContractors at any level, with the direct Government funding flowing down to such subContractors through the Contractor. The Contractor shall include this Government funding requirement in its subcontracts and shall require its subContractors to include the flow down requirement in contracts with their subContractors.
H.12	**Subject Invention Reports**
	Subject Invention Reports are required from the Contractor and subContractors IAW DFARS 252.227-7038 (large business prime Contractor) or IAW FAR 52.227-11 and DFARS 252.227-7039 (small business prime Contractor). Interim and final subject invention reports may be submitted on DD Form 882.
H.13	**Export or import authorizations**
	Should a U.S. export authorization or U.S. import authorization be required for the Contractor or a subContractor to access or receive technology, technical information, or computer software, it is solely the responsibility of the Contractor (and not the U.S. Government) to obtain that authorization. Further, such authorization must be approved and effective in a timely manner such that deadlines are met on-time.
	***** END OF NARRATIVE H0001 *****