

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD National Industrial Security Program Operating Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING	
				a. FACILITY CLEARANCE REQUIRED <b>SECRET</b>	
				b. LEVEL OF SAFEGUARDING REQUIRED <b>SECRET</b>	
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>			3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>		
	a. PRIME CONTRACT NUMBER		<b>X</b>	a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD) <b>20140617</b>
	b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>	Revision No. DATE (YYYYMMDD)
<b>X</b>	c. SOLICITATION OR OTHER NUMBER <b>W56HZV-14-R-0039</b>	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete item 5 in all cases)</i>	DATE (YYYYMMDD)
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If yes, complete the following:  Classified material received or generated under <i>Preceding Contract Number</i> is transferred to this follow-on contract.					
5. IS THIS A FINAL DD 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. If yes, complete the following:  In response to the contractor's request dated _____, retention of the identified classified material is authorized for the period of _____					
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE  <b>TBD</b>		b. CAGE CODE  <b>TBD</b>	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)  <b>TBD</b>		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)		
8. ACTUAL PERFORMANCE					
a. NAME, ADDRESS, AND ZIP CODE  <b>TBD</b>		b. CAGE CODE  <b>TBD</b>	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)  <b>TBD</b>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT  <b>Joint Light Tactical Vehicles (JLTV) Low Rate Initial Production (LRIP) and Full Rate Production (FRP) Family of Vehicles (FoV) Solicitation and proposal.</b>					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:		YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATION SECURITY (COMSEC) INFORMATION		<b>X</b>		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<b>X</b>
b. RESTRICTED DATA			<b>X</b>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<b>X</b>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			<b>X</b>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<b>X</b>
d. FORMERLY RESTRICTED DATA			<b>X</b>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<b>X</b>
e. INTELLIGENCE INFORMATION:				e. PERFORM SERVICES ONLY	<b>X</b>
(1) Sensitive Compartmented Information (SCI)			<b>X</b>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<b>X</b>
(2) Non-SCI		<b>X</b>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<b>X</b>
f. SPECIAL ACCESS INFORMATION			<b>X</b>	h. REQUIRE A COMSEC ACCOUNT	<b>X</b>
g. NATO INFORMATION			<b>X</b>	i. HAVE TEMPEST REQUIREMENTS	<b>X</b>
h. FOREIGN GOVERNMENT INFORMATION			<b>X</b>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<b>X</b>
i. LIMITED DISSEMINATION INFORMATION			<b>X</b>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<b>X</b>
j. FOR OFFICIAL USE ONLY INFORMATION		<b>X</b>		l. OTHER <i>(Specify)</i> Follow and implement:	
k. OTHER <i>(Specify)</i> <b>(1) Controlled Unclassified Information (CUI)</b> <b>(2) PM JLTV Security Classification Guide</b>		<b>X</b>		<b>(1) Threat Awareness and Reporting Requirements</b> <b>(2) JLTV Program Protection Plan</b>	<b>X</b>

DD Form 254, DEC 99

Previous editions are obsolete.

**12. PUBLIC RELEASE.** Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the National Industrial Security Program Operating Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

Direct  Through (specify):

**The PCO to the PM JLTV, ATTN: Warren, 6501 E. 11 Mile Road, CCTA-HTB-B, Mail Stop 416, The Security Manager to PM JLTV, ATTN: Security Manager, AMSTA-CSS-F / Mail Stop 105, 6501 E. 11 Mile Road, Warren, MI 48397-5000, who will obtain public release approval through the prescribed channels to include the PCO and PAO. Please refer to DFAR 252.204-7000 and Special Provision H.3**

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)\* for review.  
 \*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency

**13. SECURITY GUIDANCE.** The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

**Collateral classified information generated in support of this contract shall be classified in accordance with the source material used or the Security Classification Guide (SCG) Joint Program Office Joint Light Tactical Vehicle (JLTV) , 27 Nov 2013 and protected in accordance with the National Industrial Security Program Operating Manual (NISPOM) DoD 5220.22-M; JLTV Program Protection Plan (PPP); and, this DD Form 254. Unclassified information will be protected IAW the JLTV SCG, JLTV PPP, the OPSEC Plan, and Attachment A.**

**All classified material shall be transmitted IAW the NISPOM (Registered US Mail, cleared commercial carrier (Monday thru Thursday), Same Day Delivery, or secure fax). Access to technical data by foreign interests is prohibited unless authorized by a valid export authorization.**

**The following attachment is made part of this DD Form 254:**  
**Attachment A – Guidelines for Controlled Unclassified Information (Item 10.k., includes Item 10.j.)**  
**Attachment B – Guidelines for Communication Security (COMSEC) (Item 10.a.)**  
**Attachment C – Guidelines for Intelligence Information: Non-SCI (Item 10.e (2))**

**CUI and OPSEC requirements will be flowed down to all U.S. subcontractors (including unclassified U.S. subcontractors) as an integral part of their respective contracts.**

**UPON COMPLETION OF CONTRACT OR AT GOVERNMENT DIRECTION: All classified (CONFIDENTIAL and SECRET), or Controlled Unclassified Information (CUI) material (documents, media, hardware, software, vehicles, etc.) supplied to the contractor during the course of this contract will be destroyed according to the NISPOM or return these items to the PM JPO JLTV for destruction not later than one year after completion of contract. Contractors wishing to maintain the material for a longer period must receive permission from the Government Contracting Officer.**

**PCO concurrence:**

PELISH, BARBARA E. 1284770850

Barbara E. Pelish 17Jun2014  
**Government Contracting Officer**  
 586-282-6199

**See Continuation of Block 13**

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements, in addition to NISPOM requirements, are established for this contract. (If, Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) YES  NO

**Also see Block 13 for additional requirements.**

**15. INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use item 13 if additional space is needed.) YES  NO

**The Defense Security Service has cognizance over this contract. The Government Security Manager reserves the right to inspect compliance with the DD254, the PPP and Guidelines for CUI.**

**16. CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this contract effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL <b>Gioacchino (Jack) Ciraulo</b>	b. TITLE <b>PM JPO JLTV Security Manager</b>	c. TELEPHONE (Include Area Code) <b>586-239-3491</b>
d. ADDRESS (Include Zip Code) <b>PEO CS &amp; CSS SFAE-CSS- JL MS 640 6501 East Eleven Mile Road Warren, MI 48397-5000</b>	17. REQUIRED DISTRIBUTION <input checked="" type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input type="checkbox"/> f. OTHERS AS NECESSARY	
e. SIGNATURE 		

## CONTINUATION OF BLOCK 13 OF THE DD FORM 254

Item 10.a – COMMUNICATIONS SECURITY (COMSEC): Classified COMSEC material is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. COMSEC information/material will be accessed and/or processed IAW DoD 5220.22-M, NSA/CSS Policy Manual 3-16, AR 380-40 (Policy for Safeguarding and Controlling Communications Security), and additional security Guidelines for COMSEC (Attachment B). When access is required at Government facilities, contractor personnel shall adhere to COMSEC rules and regulations as mandated by Command policy and procedures. Contractor personnel requiring COMSEC access must be U.S. Citizens and possess a final clearance at the appropriate level. All contractors shall be briefed before access to COMSEC is granted. The contractor may be subject to the Department of Army Cryptographic Access Program (DACAP) if contractor employees handle unencrypted SECRET crypto or TOP SECRET crypto keying material. Subcontracts requiring classified COMSEC information shall be awarded only upon the written approval of the Government Contracting Officer.

Item 10.e.(2) – INTELLIGENCE INFORMATION: NON-SCI: Non-SCI Information is not releasable to contractor employees who have not received a clearance at the appropriate security level. Written concurrence of the Government Contracting Officer is required prior to subcontracting. Access to Intelligence information required for performance. Non-SCI information/material will be accessed and/or processed IAW DoD 5220.22-M, and additional security Guidelines for Intelligence Information: Non-SCI (Attachment C).

Item 10.j – FOR OFFICIAL USE ONLY (FOUO): FOUO Information generated and/or provided under this contract shall be safeguarded and marked as specified in additional Guidelines for Controlled Unclassified Information (CUI) (Attachment A).

Item 10.k.(1) – CONTROLLED UNCLASSIFIED INFORMATION (CUI) generated and/or provided under this contract shall be safeguarded and marked as specified in additional Guidelines for Controlled Unclassified Information (CUI) (Attachment A).

Item 10.k.(2) – Security Classification Guidance: J L T V SCG, 27 November 2013.

Item 11.c – RECEIVE AND GENERATE CLASSIFIED INFORMATION: The contractor requires access to classified source data up to and including Secret in support of the work effort. Any extracts or use of such data requires the contractor to apply derivative classifications and markings consistent with the source documents. Use of “Multiple Sources” on the “Derived From” line necessitates compliance with the NISPOM, paragraph 4-208a, and the use of a bibliography.

Item 11.d – FABRICATE, MODIFY OR STORE CLASSIFIED HARDWARE: Contractor must provide adequate storage at their facility for collateral classified hardware to the level of Secret.

Item 11.g – BE AUTHORIZED TO USE THE SERVICES OF THE DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER: The contractor shall prepare DD Forms 1540 and/or 2345 for authorized access to DTIC. Completed forms shall be provided to the Government Contracting Officer to verify the need-to-know and submit the DD forms on behalf of the contractor. Refer to NISPOM Chapter 11, Section 2 for more information.

Item 11.h – REQUIRE A COMSEC ACCOUNT: Contractor is authorized the use of secure telephones with fax, encryption equipment and keying material for classified program requirements.

Item 11.i – HAVE TEMPEST REQUIREMENTS: Prior to the implementation of any TEMPEST countermeasures or expenditure of funds, a TEMPEST assessment will be conducted at all contractor facilities electronically processing classified information. Each facility shall provide the following information through the government security manager (see Block 16) within 30 days of contract award. TEMPEST assessments will be marked at a minimum of FOUO 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. This requirement shall be flowed down to all U.S. subcontractors that use Information Systems to process classified material.

## CONTINUATION OF BLOCK 13 OF THE DD FORM 254

- a. Facility location—include the exact address, building number, room number, and so forth. An area map showing the facility location in relation to other buildings, perimeter, and so forth, if available.
- b. Point of contact—include the e-mail addresses and phone numbers (commercial and cell).
- c. Level of processing—include the classification level of the information that the facility will process (Secret, Top Secret, sensitive compartmented information (SCI), Special Access Program (SAP), and so forth), and frequency of processing.
- d. Foreign nationals-include if any foreign nationals work in the facility or in close proximity to the facility.
- e. Transmitters—include information on any transmitters (cell phones, two-way pagers, radios, transceivers (including alarm systems), wireless systems, portable electronic devices and repeaters) located within your facility or in close proximity (10 meters) to the facility. Include the make/model of the transmitters. Indicate how close transmitters are located to your classified processing areas.

Item 11.j – OPERATIONS SECURITY (OPSEC) REQUIREMENTS: The contractor shall follow the government program/procedures, as well as annexes and updates. The contractor is not required to develop their own OPSEC Plan. All U.S. contractors shall provide annual program specific OPSEC training for all program personnel. New program personnel shall receive OPSEC training within 30 days of program assignment. Annually, contractors shall complete OPSEC training and submit a report, validating 100% completion to the Government Security Office by 30 September. These requirements, OPSEC Plan and training, shall be flowed down to all U.S. subcontractors with access to CUI and/or classified material.

Item 11.I.(1) – THREAT AWARENESS AND REPORTING REQUIREMENTS: ICW NISPOM 1-301, the contractor shall report threat-related incidents, behavioral indicators, and other matters of counterintelligence (CI) interest specified in AR 381-12, Chapter 3, through the facility security officer to the government security officer, the nearest military CI office, the Federal Bureau of Investigation, and the Defense Security Service. Annually, train personnel who handle classified information IAW AR 381-12, Chapter 2. This requirement shall be flowed down to all U.S. subcontractors that have access to classified information/material.

Item 11.I.(2) – PROGRAM PROTECTION PLAN (PPP) – The Joint Light Tactical Vehicle (JLTV) Program Protection Plan (PPP) is effective immediately and is mandatory for use by all program participants and field activities at all program locations.

Item 12 – PUBLIC RELEASE: An electronic copy of the request with full text and graphics must be provided through the Government Contracting Officer at least forty-five (45) working days prior to the requested release date. If all or part of the information was generated by another organization, their written release authorization must accompany the request.

Notification of loss or compromise of collateral classified information shall be provided to the Government Program Security Office within 72 hours of the incident, in addition to the reporting requirements outlined in the NISPOM.

ATTACHMENT A

**ADDITIONAL GUIDELINES FOR CONTROLLED UNCLASSIFIED INFORMATION**

**General:** There are types of information that are not classified but that require application of access and distribution controls and protective measures for a variety of reasons. This information is known as "controlled unclassified information (CUI)." The types of information considered CUI for the program are information marked "For Official Use Only" by the U.S. Government and technical data. When handling CUI material, all personnel are to comply with these requirements and follow their company policy and/or applicable Proprietary Information Agreements (PIA) concerning the protection of proprietary information in situations not clearly stated herein.

**Technical Data Description:** Any recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process, or can be used to design, procure, produce, support, maintain, operate, repair, or overhaul program material. The data may be graphic or pictorial delineations in media (e.g., computer software, drawings, or photographs), text in specifications, related performance or design documents, or computer printouts. 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.

**For Official Use Only (FOUO) Information Description:** "For Official Use Only (FOUO)" is a Government designation applied to **unclassified** information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA). FOUO information includes information identified as such in the Security Classification Guide or information from a government document marked FOUO.

**CUI Markings**

Marking of FOUO documents will be in accordance with Army Regulation (AR) 25-55. Information extracted from an FOUO document will carry the FOUO marking until formally reviewed by the government. AR 25-55 can be found at [http://www.apd.army.mil/pdffiles/r25\\_55.pdf](http://www.apd.army.mil/pdffiles/r25_55.pdf).

Marking of Technical Data will include the statement provided in the Security Classification Guide. 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.

**Protection of CUI Information**

**Access:** CUI may be released only to an individual who has a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. Information in any media format may only be disseminated on a need-to-know basis. The need-to-know restricts the use or dissemination of CUI data to those individuals or organizations with direct affiliation with the given program or project. Further dissemination of such information will be at the discretion of the Government Security Manager. Personnel no longer requiring access to CUI must delete or surrender any in their possession and terminate future access to it.

**Storing/Handling:** During working hours, take reasonable steps to minimize risk of access to CUI by unauthorized personnel. After working hours, store CUI information in locked desks, file cabinets, bookcases, locked rooms, or similar means. Do not display CUI in public places (e.g., airports, airplanes, restaurants). Computers used to process CUI do not need to be accredited for classified use. Do not process CUI on public computers (e.g., those available for use by the general public in kiosks, hotel business centers) or computers that do not have access control. Personally owned computers are not authorized to process CUI. Mobile devices used to store CUI electronically (e.g., company-issued laptops, personal electronic devices [PED], removable media) must be physically protected and use NIST/NIAP-approved cryptographic products. These are available at <http://iase.disa.mil/pki/eca> or <http://csrc.nist.gov/cryptval/>.

**Dissemination:** CUI printed documents and material may be transmitted through mail channels or hand-carried without formal courier orders. FOUO information may be disseminated to DoD personnel and DoD contractors to conduct official business for the program. If dissemination is required outside of DoD personnel or DoD contractors, contact the Government Security Manager for approval. Technical data will follow the release instructions identified in the Distribution Statement. Use secure communications whenever possible; however, land-line telephones are more secure than cellular telephones and should be used whenever available for discussions involving CUI. Transmit voice and facsimile transmissions only when you have a reasonable assurance that only authorized recipients will have access to the transmission. Digital transmission shall comply with the below:

## CONTINUATION OF BLOCK 13 OF THE DD FORM 254

- All transmission and/or dissemination of CUI identified with a Distribution Statement or marked "FOUO" (i.e., email and file transfers) must use NIST/NIAP-approved cryptographic vendors and algorithms, e.g., DoD-approved Public Key Infrastructure Certification. These are available at <http://iase.disa.mil/pki/eca> or <http://csrc.nist.gov/cryptval/>. This encryption requirement includes passcodes to teleconferences or web conferences where there is a reasonable expectation that CUI may be discussed. When encryption is not available, a government collaborative suite (aka Integrated Digital Environment [IDE]) must be used to transmit CUI. Encrypt all wireless external data connections.
- Award contractors. Contractor personnel required to send FOUO information via email will maintain an email encryption capability with Government counterparts. The DoD has established the External Certification Authority (ECA) program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to encrypt email to JLTV and authenticate to JLTV Information Systems. Provided is the link where contractors can get certificates that allow encryption without a CAC: <http://iase.disa.mil/pki/eca/>
- Contractor-hosted collaborative suites may be used for digital transmission and/or dissemination of CUI by personnel not located on a government backbone (e.g., NIPRNET), provided the following conditions apply:
  - Use only NIST/NIAP-approved cryptographic vendors and algorithms. The latest validation lists may be obtained at <http://iase.disa.mil/pki/eca> or <http://csrc.nist.gov/cryptval/>.
  - Use an internally hosted service that does not use a third-party collaborative suite service provider.
- All computers containing CUI must be either protected by physical isolation from all personnel without a valid need for the information or protected using NIST/NIAP-approved cryptographic products. Discretionary access control measures must be used to preclude access to CUI by users who are not authorized access to CUI. After working hours, when not in physical possession of the owner, all electronic assets containing CUI must be afforded a reasonable degree of physical protection to prevent theft of program information (e.g., locking up laptops or cable locking them to a stationary base, storing in trunk, or storing out of sight).
- Do not post CUI to web pages that are publicly available or have access limited only by domain/IP restrictions. As permitted by other contract provisions, CUI may be posted to web pages that control access through the use of a DoD approved Public Key Infrastructure Certification and that provide protection via use of secure sockets, or other equivalent technologies. These are available at <http://iase.disa.mil/pki/eca>.
- As new technologies become available in the electronics arena, care should be given to providing a reasonable degree of protection from known vulnerabilities.
- The Internet is "Public Access". CUI must be reviewed and officially approved by the PEO GCS Public Affairs Officer for public release before placing on the Internet. This is not applicable when the Internet is used for e-mail transmissions and encryption is used as noted above.

**Disposal:** Destroy CUI documents by any means approved for the destruction of classified information, i.e. cross-cut shredding or other means that would make it difficult to recognize or reconstruct the information. Clear, purge, or destroy CUI on removable media IAW BBP 03-PE-O-0003 Army Information Assurance Sanitization of Media to AR 25-2. This is available at <https://informationassurance.us.army.mil>.

**Report of Loss of CUI:** Report any loss of CUI or loss of CUI from a contractor information system that is known to the contractor within the period of performance of this contract to the Government Security Manager. Initial reports shall be made as expeditiously as possible in all cases within 72 hours of discovery. If additional information is required after submission and review of the initial report, guidance will be provided at that time. Mark any reports For Official Use Only, exemptions 2 and 5 apply. Initial report content shall include the following information as available.

- Applicable dates, including dates of compromise and dates of discovery
- Threat methodology, including all known resources used (e.g. IP addresses, domain names, software tools)
- Account of what actions the threat(s) may have taken on victim system/network
- What information may have been compromised, exfiltrated, or lost, and its potential impact on government programs

**Report of Cyber Intrusions:** Report cyber intrusions or other compromises of CUI to your supporting counterintelligence office, which will inform the DoD-DIB Common Information Sharing Environment (DCISE). Notify the Government Security Manager of any incidents as well. Refer to Report of Loss of CUI for what needs to be reported, when, and how.

## CONTINUATION OF BLOCK 13 OF THE DD FORM 254

### ATTACHMENT B: ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Contractor Generated Communications Security (COMSEC) Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the Contracting Officer, or his/her duly appointed representative.

#### REQUIREMENTS:

1. The requirements of DoD 5220.22-M and NSA/CSS Policy Manual 3-16 are applicable to this effort.
2. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA.
3. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
4. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement "Not Releasable to the Defense Technical Information Center per DoD Directive 5100-38."
5. Classified paper COMSEC material may be destroyed by burning, disintegration, chopping or high security crosscut shredding. Cryptographic key tapes must be "terminally" destroyed (destroyed to the point where it cannot be reconstructed) utilizing devices listed on the Evaluated Products List (EPL) for Punched Tape Destruction Devices or the EPL for High-Security Disintegrators. A listing of EPLs can be found at <http://www.nsa.gov/ia/government/mdg.cfm>. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
6. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without the express written permission of the Director, NSA, is strictly prohibited.
7. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the government security manager.
8. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:
  - a. "COMSEC MATERIAL - ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."
  - b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA"

## CONTINUATION OF BLOCK 13 OF THE DD FORM 254

### ATTACHMENT C: INTELLIGENCE INFORMATION: NON-SCI

*Intelligence information includes the following information (whether written or in any other medium) classified pursuant to Executive Order 12333: Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from U.S. intelligence efforts; and information on Intelligence Community protective security programs (e.g., personnel, physical, technical, and information security).*

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the TACOM Life Cycle Management Command (TACOM LCMC) G2 Foreign Intelligence Team. Any intelligence materials so provided will be disseminated solely by the G2 TACOM LCMC, and will be accompanied by both a Letter of Instruction governing control of the materials provided, and a Letter of Transmittal, identifying the materials loaned and the duration of the loan. This service only pertains to elements supported by the G2 TACOM LCMC.
2. All requests for access to intelligence materials will adhere to the following guidelines:
  - a. Prime contractor requests for intelligence materials access will be sent to the Program/Project Manager (PM) of the User Activity on official business letterhead with an enclosed copy of the approved DD Form 254.
  - b. Subcontractor requests for access to intelligence materials will be forwarded by the prime contractor to the PM on official business letterhead with an enclosed, approved DD Form 254 for the relevant subcontract.
  - c. PM of the User Activity will forward request through the Contracting Officer on official letterhead with the appropriate DD Form 254 and all substantiating documents attached, to be forwarded to the G2 TACOM LCMC for review and concurrence.
3. The handling of all non-SCI intelligence material will follow NISPOM need-to-know requirements for all PEO Ground Combat Systems locations as authorized on their DD-254's. Any intelligence material that does not fall under the NISPOM need-to-know will be clearly identified as an exception by the Foreign Intelligence Officer (FIO) or Threat Manager (TM). Such material will contain handling instructions, i.e. safeguarding, transmitting, and disseminating.
4. The contractor shall not release intelligence information to foreign nations, foreign companies, foreign corporations or foreign subsidiaries or other non-U.S. citizens. If a need arises for the release of intelligence information, the contractor will request such release in writing to the FIO or TM who in turn will process the request through proper foreign disclosure channels.
5. Upon expiration of the contract, the intelligence inventory will be submitted to the FIO or TM with the recommended disposition of intelligence materials (i.e. retention, transfer to another contract, destroy in place, return).
6. The U.S. Army Tank-automotive and Armaments Command, G2, Foreign Intelligence Office will maintain the list of supporting FIOs and TMs authorized to release intelligence information to the company. The primary supporting Intelligence Specialist, G2, TACOM is the Foreign Intelligence Team member with the following contact information:

FIO POC: **Guy Flummerfelt**

POC Phone: **586-282-6262**

Supporting PM Office: **PM JPO JLTV**

U.S. Army Tank-automotive and Armaments Command  
ATTN: Foreign Intelligence Officer for PM JPO JLTV  
AMSTA-CSS-F / mail stop 105  
6501 E. 11 Mile Road  
Warren, MI 48397-5000