DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Secret

b. LEVEL OF SAFEGUARDING REQUIRED: Secret

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: W56HZV-12-R-0445	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*
	b. REVISED *(Supersedes all previous specs)*	REVISION NO.	DATE *(YYYYMMDD)*
	c. FINAL *(Complete Item 5 in all cases)*		DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
To be announced		To be announced

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Solicitation for the Production and Deployment (PD) Phase of the Bridge Erection Boat (BEB) Program.

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		X
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT		X
g. NATO INFORMATION		X	i. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER *(Specify)*		X
k. OTHER *(Specify)*		X			

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security 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 [X] Through *(Specify)*

Contracting Officer, Army Contracting Command - Warren, 6501 E 11. Mile Road, Warren, MI 48397-5000

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.)*

PEO CS&CSS Armoring Systems Security Classification Guide effective 31 Aug 2012.

- S -
RAND PONTING
System Acquisition Manager
PM Bridging
16 January 2013

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [ ] Yes [X] No
(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.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [X] No
(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.)

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

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*
Gregg Schamel	Security Specialist	(586) 282-6341

d. ADDRESS *(Include Zip Code)*	**17. REQUIRED DISTRIBUTION**
6501 E. 11 Mile Rd Warren, MI 48397	[ ] a. CONTRACTOR [X] b. SUBCONTRACTOR [X] c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	[ ] d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION [X] e. ADMINISTRATIVE CONTRACTING OFFICER [ ] f. OTHERS AS NECESSARY

DD 254, Item 13 Continuation Sheet

The security classification guide for this Contract is Combat Support & Combat Service Support Armoring Systems SCG FOR dated 31 Aug 2012, PEO CS and CSS. .

The Contractor will comply with all of the security requirements in DOD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

CLASSIFIED INFORMATION HANDLING

1. Employees of the contractor may act as couriers for classified material. All classified material will be transmitted IAW the NISPOM (Registered US Mail, cleared commercial carrier (Monday thru Thursday), Same Day Delivery, SIPRNET, or secure fax.)

2. All classified material (CONFIDENTIAL and SECRET) supplied to the contractor during the course of this program will return these items to the G2, TACOM, LCMC for destruction not later than 1 year after termination on the contract.

Attn G2, TACOM, LCMC
AMSTA-CS-S
6501 E. 11 Mile Rd/Mail Stop #105
Warren, MI 48397

3. Contracts are required to establish means to control classified information. This will include maintaining receipts (DA 3964) of all classified material shipped or received that is associated with this solicitation.

4. GSA approved security containers are required to store classified material. Contractors will ensure all personnel who perform maintenance on any security container storing classified information are cleared to the SECRET level.

5. Any contractor who wishes to hold meetings in which classified information will be discussed are required to do so either on federal installations or a cleared facility. They should contact TACOM G2 for approval of meeting locations for CONUS locations.

6. In the event of a possible compromise of classified information under the control of the contactor, the contactor will immediately notify DSS; and his local security support office.

INFORMATION AND COMPUTER SECURITY

1. The contractor will not transmit any FOUO information electronically over the Internet unless it is encrypted by FIPS 140-2 standard. Alternative dissemination methods include: secure fax; US mail; and hand carrying FOUO material. FOUO information maybe disseminated by vendor's internal computer network if its protected with a firewall and individual access is controlled by using IDs and passwords.

2. All classified material received will be handled and stored IAW with NISPOM. Any computer used by the contractor to process classified information must have a written accreditation. For CONUS the contractor obtains an accreditation from the Cognizant Security Office (DSS). The contractor must provide a copy of there accreditation certificate from DSS to the G2 TACOM prior to processing any classified information. If working in a government controlled office the government will be responsible form maintaining accreditation records. All computers will be marked with the appropriate visual markings showing what level of classified information may be processed on the computer (e.g. Secret, Confidential, and unclassified). All storage media will be marked to reflect the highest classification level of the system accreditation irrespective of what is saved on the storage device (SECRET).

3. When processing classified information on a computer, the contractor will ensure he/she does so in a secure environment. Continuous supervision will be required to ensure inadvertent access to classified does not occur. All personnel with access to the computer must have a SECRET clearance and a need to know.

4. If classified computer processing is required, the contractor will contact DSS to initiate a TEMPEST countermeasures review to evaluate what TEMPEST measures are required if any. This only applies to computers solely operated by the contractor or CONUS offices.

5. Cell phones, Palm Pilots, pagers, and beepers etc will not be operated in areas approved for classified computer processing.

OPSEC

1. If the contractor generates unclassified OPSEC sensitive information, this information will be protected at the same level as FOUO information. The contractor will not transmit any OPSEC sensitive information electronically over the Internet unless it is encrypted IAW FIPS 140-2 standard. Alternative dissemination methods include secure fax, US mail, and hand carrying OPSEC sensitive material. OPSEC sensitive information maybe disseminated within the contractors internal computer network if it is protected with a firewall and individual access is controlled by using IDs and passwords. (Under no circumstances can classified information be transmitted over an unclassified network.)

2. The contactor may disseminate "FOR OFFICIAL USE ONLY" (FOUO) information to their employees who have a need to know for the information in connection with the purchase order.

3. All FOUO material will be destroyed by tearing or shredding to make unreadable. Electronic media will be purged with approved software or destroyed through a physical process.

4. Examples of information that would be considered OPSEC sensitive:

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

5. All unclassified technical documents generated in connection with the PO will be marked as **Distribution Statement C**: Distribution authorized to US government agencies and contractors associated with PEO CS and CSS and TACOM Life Cycle Management Command (LCMC) locations or providing support to the TACOM LCMC and community partners IAW AR 530-1. For Official Use Only (FOUO) caveat is assigned so as not to place US personnel at risk, or compromise security procedures, or DoD information (Critical Technology). This document is not releasable to the public or media. Destroy by shredding or tearing to make unreadable, when no longer needed. This document should not be sent over the INTERNET unencrypted, or posted to any public web sites. Other requests for this document shall be referred to Contracting Officer, Army Contracting Command, 6501 E 11 Mile Road, Warren, MI 48397).

6. All information pertaining to this contract which is being considered for public release will undergo an OPSEC review using the TACOM LCMC OPSEC review process (STA Form 7114,) prior to release. A copy can be found in the back of the CS & CSS Armoring SCG

7. The "FOR OFFICIAL USE ONLY" marking is assigned to information at the time of its creation in a DOD User Agency. It is not authorized as a substitute for a security classification marking but it is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

8. Other non-security markings such as "Limited Official Use" and "Official Use Only" are used by non-DOD Users Agencies for the same type of information and should be safeguarded and handled in accordance with instructions received from such agencies.

9. Use of the above markings does not mean that the information cannot be released to the public, only that it must be reviewed by the Government prior to its release, to determine whether a significant and legitimate Government purpose is served by withholding the information portions of it.