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: N/A

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

	a. PRIME CONTRACT NUMBER		
	b. SUBCONTRACT NUMBER		
X	c. SOLICITATION OR OTHER NUMBER: W52P1J-10-R-1055	DUE DATE *(YYYYMMDD)*	

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

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*: 20100507
	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)*
		Defense Security Service

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Hawthorne Army Depot 1 South Maine Avenue Hawthorne, NV 89415-9404		Defense Security Service (S41PX) 10040 N. 25th Avenue, Suite 118 Phoenix, AZ 85021-1647

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Operation and maintenance of Hawthorne Army Depot

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)		X	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI		X	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)* Controlled Unclassified Information (CUI)	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)*

US Joint Munitions Command Public Affairs Office (AMSJM-PA)
1 Rock Island Arsenal
Rock Island, IL 61299

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.)*

Classified material must be handled IAW the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M (Feb 06), Department of the Army Information Security Program, AR 380-5 (29 Sep 2000), any local security classification guidance and source documents. Applicable Security Classification Guidance will vary depending on the information accessed. The ACC RICC PCO must be notified and approve the receipt and/or generation of classified information.

Remaining Security requirements continued on attachment, DD Form 254, Block 13 - continued.

Certification and signature: Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this effort. All questions shall be referred to the officials as identified below.

Barbara J Hansen

Barbara Hansen, Procuring Contracting Officer
U.S. Army Contracting Command/Rock Island Contracting Center
Rock Island, IL 61299-8000
309-782-8662/DSN 793-8662

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] Yes [ ] 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.)

HS 7001, Operations Security (OPSEC) Requirements, Jan 09 including CDRL and DiD (DI-MGMT 80934A), in addition to supplemental guidance listed under Block 13.

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)*
Judy R. Orasky	Industrial Security Specialist	309-782-8336/DSN 793-8336

d. ADDRESS *(Include Zip Code)*
HQ US Army Joint Munitions Command
ATTN: AMSJM-FP
Rock Island, IL 61299

e. SIGNATURE
Judy R Orasky

17. REQUIRED DISTRIBUTION

- [X] a. CONTRACTOR
- [ ] b. SUBCONTRACTOR
- [X] c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
- [ ] d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
- [X] e. ADMINISTRATIVE CONTRACTING OFFICER
- [ ] f. OTHERS AS NECESSARY

DD Form 254, Block 13 – continued for Solicitation W52P1J-10-R-1055

Block 10j. – FOR OFFICIAL USE ONLY (FOUO): FOUO is applied to information that may be exempt under one or more of the nine exemptions under the Freedom of Information Act (FOIA).

a. No person may have access to information designated as FOUO unless that person has been determined to have a valid need for such access in connection with the accomplishment of a lawful and authorized Government purpose. The final responsibility for determining whether an individual has a valid need for access to FOUO information rests with the individual who has authorized possession, knowledge or control of the information and not on the prospective recipient.

b. Information designated as FOUO may be disseminated within the Department of Defense Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the DoD, provided that dissemination is not further controlled by a Distribution Statement.

c. During working hours, reasonable steps shall be taken to minimize risk of access by unauthorized personnel. After working hours, store FOUO information in unlocked containers, desks or cabinets if Government or Government-contract building security is provided. If such building security is not provided, store the information in locked desks, file cabinets, bookcases, locked rooms, etc.

d. FOUO information and material may be transmitted via first class mail, parcel post or, for bulk shipments, via fourth class mail. Electronic transmission of FOUO information, e.g., voice, data or facsimile, e-mail, shall be by approved secure communications systems or systems utilizing other protective measures such as encryption or Public Key Infrastructure (PKI), whenever practical.

e. FOUO information may not be released to publicly accessible web sites. It may only be posted to DoD Web sites consistent with security and access requirements specified in the Assistant Secretary of Defense (C3I) Memorandum dated November 1998, Subject: "Web Site Administration Policies and Procedures".

f. FOUO documents may be destroyed by any of the means approved for the destruction of classified information, or by any other means that would make it difficult to recognize or reconstruct the information.

g. Appropriate administrative action shall be taken to fix responsibility for unauthorized disclosure of FOUO whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act may also result in civil and criminal sanctions against responsible persons. The Military Department or other DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

DD Form 254, Block 13 – continued for Solicitation W52P1J-10-R-1055

Block 10k. – Other - Controlled Unclassified Information (CUI): Controlled Unclassified Information is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces "Sensitive but Unclassified" (SBU). Within the DoD, the criteria for allowing access to CUI information are the same as those used for FOUO information, except that information received from the Department of State marked SBU shall not be provided to any person who is not a US citizen without the approval of the Department of State activity that originated the information.

Block 11.a. – Have Access to Classified Information Only at Another Contractor's Facility or a Government Activity: Contract performance is restricted to Hawthorne Army Depot, Hawthorne, NV.

Block 11.c. - Receive and Generate Classified Material: All classified information received or generated under this contract is the property of the US Government. At the termination of expiration of this contract, the US Government will be contacted for proper disposition instructions. Prior to granting an employee access to classified materials, you will brief the employee on his obligation to safeguard the information. The appropriate portion of SF312, "Classified Information Non-Disclosure Agreement", will be executed at the time of briefing. If access to SIPRnet and INTELINK-S is granted, the following guidelines apply:

a. The computer account will be used in support of an official government project.

b. You will not willfully compromise the account password.

c. You will notify the Contracting Officer's Representative (COR) when the account is no longer needed, or account information needs revising, or the account password has been knowingly compromised.

d. The account will be used in accordance with all existing instructions, policy directives, and guidelines to ensure no improper or fraudulent use.

e. Data and files associated with this account are subject to random review.

f. The account password will be changed in accordance with current Army policy.

g. You are responsible for not only safeguarding the classified contents of this account, but also the physical configuration of the network.

DD Form 254, Block 13 – continued for Solicitation W52P1J-10-R-1055

Block 11.d. – Fabricate, Modify or Store Classified Hardware: Contractor must provide adequate storage for classified hardware to the level which exceeds two cubic feet but not more than 66 cubic feet.

Block 11.j. – Operations Security (OPSEC) Requirements:

a. As defined in Army Regulation (AR) 530-1, Operations Security (OPSEC), **sensitive information** is information requiring special protection from disclosure that could cause compromise or threat to our national security, an Army organization, activity, family member, DA civilian or DoD contractor. **Critical Information** is defined as information important to the successful achievement of U.S. objectives and missions, or which may be of use to an adversary of the United States. It consists of specific facts about friendly capabilities, activities, limitations (includes vulnerabilities), and intentions needed by adversaries for them to plan and act effectively so as to degrade friendly mission accomplishment. All critical information is sensitive, but not all sensitive information is critical.

b. The Contractor shall not release sensitive information to the general public without prior written approval from the Contracting Officer. All contractor requests to release sensitive information shall be in writing and clearly explain the necessity for release of the information and consequences if approval is not granted. Contractor employees who are U.S. citizens shall be provided access to sensitive information on a "need to know" basis required to fulfill the terms and conditions of the contract. Foreign National (FN) employees' access to information will be limited to non-sensitive information. FN access to sensitive information will be approved in writing by the Contracting Officer on a case-by-case basis, and will be strictly limited to the information that the employee must know in order to fulfill the terms and conditions of the contract.

c. The Contractor shall be responsible for establishing and maintaining an OPSEC program to adequately manage, protect and control sensitive information that has been provided or generated under the contract. The Contractor shall appoint an OPSEC Officer to manage the OPSEC program and to prepare a written OPSEC Plan, which identifies the CI, threat information and OPSEC measures used to mitigate known vulnerabilities and risks.

d. The Contractor shall provide OPSEC training to all employees regarding the safeguarding of sensitive information prior to employees being allowed access to such information, and annually thereafter.

e. The Contractor shall destroy all sensitive program material at the completion of the contract so as to ensure the information cannot be accessed or utilized for any purpose and notify the Contracting Officer in writing of its destruction.

f. These same requirements will flow down to all subcontractors working on or provided any sensitive information related to the contract.