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: None

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

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: W52P1J-14-R-0059	DUE DATE *(YYYYMMDD)*

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

X	a. ORIGINAL *(Complete date in all cases)*		DATE *(YYYYMMDD)*: 20140102
	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)*
TBD		TBD

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)*
Multiple locations - See Block 13.		

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

The Enterprise Resource Planning (ERP) Enterprise Application Services acquisition will enable developing a Government organic capability to design and sustain Enterprise software systems. Enterprise Application Services includes the design, implementation and sustainment of ERP and enterprise systems.

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)*		X	HSPD-12 Antiterrorism Level I training		

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)*

Public Release POC: PEO EIS HQS PAO
Classified Materials Not Authorized for Release.

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.)*

NOTE: Unclassified Task Orders (TO) do not require a DD Form 254

This DD Form 254 does not authorize classified work to be performed. This DD Form 254 details the scope of classified work that may be performed under individual TOs; Each classified TO will be required to have a DD Form 254 with the appropriate security requirements (i.e. Secret). Individual classified TOs shall contain a DD Form 254 outlining the level of classification and instructions applicable to the individual TOs. Specific instructions will be provided with each classified TO. Secret is the highest classification anticipated under this contract. Classified TO Requirements are:

A. Contractors will comply with the threat awareness and reporting requirements as specified in AR 381-12, paragraph 1-14 and Chapter 3.

B. The National Industrial Security Program Operating Manual (NISPOM) January 28, 2006 to latest edition.

C. Personnel performing on this contract must be U.S. Citizens.

D. Personnel performing on the classified TOs of this contract shall be listed in the Joint Personnel Adjudication Systems (JPAS) with an owning or servicing relationship with the contract company and show proper access level up to Secret. Positions will be identified as to which eligibility applies. The investigative basis for personnel Security clearances should be IAW existing DoD Policy and AR 25-2. Contractors shall not be allowed access to classified and sensitive material until required investigations are submitted and favorable results are received.

E. PEO EIS Project Offices will provide security classification guidance for the performance of this contract. Submit visit requests to the COR and PEO EIS Security Management Office for need-to-know verification.

F. All contractors must comply with AR 25-2; Take the U. S. Army's Annual Information awareness training and any other U.S. Army training as requested.

G: See attachment 1 for additional Security Guidance for Classified TOs.

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.)

Contractors are required to have OPSEC training IAW AR 530-1, chapter 4-2. PEO EIS or another government agency may provide the OPSEC training.

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)*

d. ADDRESS *(Include Zip Code)*	**17. REQUIRED DISTRIBUTION**	
	X	a. CONTRACTOR
	X	b. SUBCONTRACTOR
	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	X	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	X	e. ADMINISTRATIVE CONTRACTING OFFICER
	X	f. OTHERS AS NECESSARY PEO EIS Industrial Security Manager

Attachment 1

Item 13 Security Guidance

Reference DD for 254 Blocks:

- 8(a) The location for the majority of work for this contract is Picatinny Arsenal, NJ and the National Capital Region (NCR). Other work locations and associated travel will include, but not be limited to: Fort Lee, VA; Radford, VA; Marlton, NJ; and Huntsville, AL.

- 10(j) Projection of For Official Use Only (FOUO) information, contractual, and Privacy Act information. FOUO information shall be marked and protected IAW AR 25-55 (Freedom of Information Act Program) and Chapter 5, AR 380-5 (DA Information Security Program). See Attachment #2 Safeguarding "For Official Use Only" (FOUO) information. Personally Identifiable Information (PII) shall be protected IAW the Privacy Act (5 USC 552a), AR 25-1, and DODI 8500.2 Information Assurance (IA) implementation.

- 11(a) Access to classified information is restricted to properly accredited Government activities. The contractor will not be required to have any safeguarding capability at its facility. Secret clearance is required to access classified information. The using activities PEO EIS government personnel will provide security classification guidance for the performance of this contract. Classified Materials/Information will be protected IAW AR 380-5.

- 11(e) The IT services that will be required consist of requirements for design, development, realization, deployment and sustainment/optimization of PEO EIS products and services.

- 11(l) The contractor shall comply with agency personal indentity verification procedures identified in the contract that implement Homeland Security Presidential Directives -12 (HSPD-12), Office of Management and Budget (OMB) Guidance M-05-24, Federal Information Processing Standards Publication (FIPS PUB) number 201 and GSA HSPD-12, Standard Operating Procedure (SOP), Personnel Security Process, dated November 18, 2005.

AR 530-1 provides basic guidance on OPSEC. Contractor personnel shall be familiar with and comply with all Government requiring activity's OPSEC policy and procedures at work locations and visiting sites. Government personnel will provide OPSEC training. See Block 14.

Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort.

Attachment #2

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

1. The "FOR OFFICAL 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 is used on official Government Information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act.

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

3. 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 informational portions of it.

4. INDENTIFICATION MARKINGS:

a. An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" at the bottom of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside of the back cover (if any). No portion marking will be shown.

b. Within a classified document, an individual page that contains FOUO and classified information will be marked at the top and bottom with the highest security classification appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked "FOUO".

c. Any "FOR OFFICIAL USE ONLY" information release to a contractor by DOD User Agency is required to be marked with the following statement prior to transfer:

THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FOIA, EXEMPTIONS APPLY.

d. Removal of the "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authorities. When "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent possible.

5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.

6. STORAGE: During working hours "FOR OFFICIAL USE ONLY" information shall be placed in an out-of-sight location if the work area is accessible to persons who do not have a need for the information. During non-working hours, the information shall be stored to preclude unauthorized access. Filing such material with other unclassified records in unlocked files or desks is adequate when internal building security is provided during non-working hours. When such internal security control is not

exercised, locked buildings or rooms will provide adequate after hours protection or the material can be stored in locked receptacles such as file cabinets, desks or bookcases.

7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-class mail.

8. DISPOSITION: When no longer need, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a trash container or as directed by the User Agency.

9. UNAUTHORIZED DISCLOSURE: Unauthorized disclosure of "FOR OFFICIAL USE ONLY" information does not constitute a security violation, but the releasing agency should be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.