

<b>DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b> <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				<b>1. CLEARANCE AND SAFEGUARDING</b>	
				a. FACILITY CLEARANCE REQUIRED <div style="text-align: center;">Top Secret</div>	
				b. LEVEL OF SAFEGUARDING REQUIRED <div style="text-align: center;">N/A</div>	
<b>2. THIS SPECIFICATION IS FOR:</b> <i>(X and complete as applicable)</i>			<b>3. THIS SPECIFICATION IS:</b> <i>(X and complete as applicable)</i>		
<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER <div style="text-align: center;">W900KK-09-D-0006</div>		<input checked="" type="checkbox"/>	a. ORIGINAL <i>(Complete date in all cases)</i> <div style="text-align: right;">DATE (YYYYMMDD) 20090804</div>	
	b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)
	c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i> <div style="text-align: right;">DATE (YYYYMMDD)</div>	
<b>4. IS THIS A FOLLOW-ON CONTRACT?</b> <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.					
<b>5. IS THIS A FINAL DD FORM 254?</b> <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 classified material is authorized for the period of _____.					
<b>6. CONTRACTOR</b> <i>(Include Commercial and Government Entity (CAGE) Code)</i>					
a. NAME, ADDRESS, AND ZIP CODE Electronic Consulting Services, Inc. 2750 Prosperity Avenue, Suite 510 Fairfax, VA 22031		b. CAGE CODE ITIE5	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Defense Security Service (S51FX2) 14428 Albemarle Point Place, Suite 140 Chantilly, VA 20151		
<b>7. SUBCONTRACTOR</b>					
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
<b>8. ACTUAL PERFORMANCE</b>					
a. LOCATION US Army Program Executive Office Simulation, Training and Instrumentation (PEO STRI) 12350 Research Parkway Orlando, FL 32826		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Defense Security Service (S21ME) P.O. Box 254036 Patrick AFB, FL 32925-0036		
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b> Systems Engineering and Technical Assistance (SETA) is a non-personal support services for program management, planning, design, development, engineering, implementation, logistics, evaluation, sustainment, operations and support acquisition, and ancillary services to PEO SRTI and other federal agencies worldwide.					
<b>10. CONTRACTOR WILL REQUIRE ACCESS TO:</b>					
	YES	NO	<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		<input checked="" type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input checked="" type="checkbox"/>	
b. RESTRICTED DATA		<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY		<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<input checked="" type="checkbox"/>
d. FORMERLY RESTRICTED DATA		<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input checked="" type="checkbox"/>	
(2) Non-SCI	<input checked="" type="checkbox"/>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>	
f. SPECIAL ACCESS INFORMATION		<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>
g. NATO INFORMATION		<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION		<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION		<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>		l. OTHER <i>(Specify)</i>	<input checked="" type="checkbox"/>	
k. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/>	See item #13		

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  Through (Specify)

US Army PEO STRI (Public Affairs Office) and Contracting Officer's Representative  
12350 Research Parkway 12350 Research Parkway  
Orlando, FL 32826-3276 Orlando, FL 32826-3276

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.)

\*\*\*For questions concerning this DD254 please contact Tom Milton (407) 208-3058\*\*\*

"SEE BLOCK 13 CONTINUATION SHEET."

CERTIFICATION AND SIGNATURE: Security requirements stated herein are complete and adequate for safeguarding the classified information to be received and generated under this classified effort. All questions should be referred to the officials

(b) (6) [Redacted Signature]

10 Aug 09

Contract Support Element (CSE)

(b) (6) [Redacted]

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

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office.  Yes  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) (6)  
b. TITLE: Contracting Officer's Security Representative  
c. TELEPHONE (Include Area Code): (b) (6)

d. ADDRESS (Include Zip Code):  
US Army PEO STRI Security Office  
12350 Research Parkway  
Orlando, FL 32826

17. REQUIRED DISTRIBUTION

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

[Handwritten Signature]

**US ARMY SCI ADDENDUM TO DD FORM 254 7 APR 09**

**XXX** (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff (DCS), G-2 as the Cognizant Security Authority (CSA) for the US Army, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DoD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SCI, and are part of the security classification specification for this contract:

**XXX** DoD 5105.21-M-1, SCI Security Manual, Administrative Security

**XXX** Signals Intelligence Security Regulations (SISR) (Available from the CM)

**XXX** Imagery Policy Series (Available from the CM)

\_\_\_\_\_ DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems

\_\_\_\_\_ DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

**XXX** AR 25-2, Information Assurance

**XXX** AR 380-28, DA Special Security System

\_\_\_\_\_ AR 380-381, Special Access Programs (SAPS).

**XXX** Army Handbook for SCI Contracts.

**XXX** Other National Industrial Security Program Operating Manual Supplement, DoD 5220.22M

**XXX** (2) Contract estimated completion date: 4 August 2010, with 4 additional one-year options if exercised. See individual orders for delivery order completion date

**XXX** (3) The name, telephone number, and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is:

FOR PM ITTS TSMO:

FOR PM CATT SOF:

<p>(b) (6)</p> <p>Acting Chief, Program Support Division Threat Systems Management Office Attn: SFAE-STRI-PM-ITTS-S Building 4497 Digney Road Redstone Arsenal, AL 35898-7461</p> <p>(b) (6)</p>	<p>(b) (6)</p> <p>Deputy Product Manager for Special Operations Training Systems Attn: SFAE-STRI-PM-CATT-STC 12350 Research Parkway Orlando, FL 32826-3276</p> <p>(b) (6)</p>
--	---

(The Contract Monitor and the contractor security officer must be registered in the Army Contractor Automated Verification System (ACAVS) in order to process SCI actions)

**XXX** (4) All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the CM for approval and then to HQ INSCOM, ACofS Security, G2, Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

**XXX** (5) The contractor will submit the request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the Contractor Support Element at least ten (10) working days prior to the visit. Visit certification requests will be processed through ACAVS.

**XXX** (6) The contractor will not reproduce any SCI related material without prior written permission of the CM.

\_\_\_\_\_ (7) Security Classification Guides or extracts are attached or will be provided under separate cover.

\_\_\_\_\_ (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3 and AR 25-2 (Note: Check only if item 11I indicates that a requirement exists for SCI AIS processing.)

\_\_\_\_\_ (9) This contract requires a contractor SCIF.

**XXX** (10) This contract requires X(SI) X(TK) \_\_ (G) \_\_ (HCS) (Add others as required)

**XXX** (11) The contractor will perform SCI work under this contract at the following locations: FOR PM ITTS TSMO: SCI Access will be granted at TSMO facilities only. FOR PM CATT SOF: Ft. Campbell, KY.

**ITEM 13 SECURITY GUIDANCE:**

1. The following items apply to this contract.

**GENERAL GUIDANCE:**

1. The contractor shall comply with (1) the Security Agreement (DD Form 441) including the National Industrial Security Program Operating Manual (DoD 5220.22-M) and (2) any revisions to that manual, notice of which has been furnished to the contractor.
2. The contractor's employees requiring access to government or another cleared contractor's facilities where proof of a security clearance is required, the contractor shall meet the security access requirements specified by the host and/or owner of those facilities.
3. The contractor shall not disclose classified or unclassified information pertaining to this contract to the public, without prior review and approval. Requests for public release shall be submitted 10 working days in advance to the address specified in block 12.
4. Prior to granting an employee access to classified materials, the contractor shall brief employees with regard to their obligation to comply with the terms of this document. The contractor's employees shall be debriefed when access to the material is terminated. A list of all employees who have had access to the classified information during the performance period of this Delivery Order shall be maintained by the company and be available for Defense Security Service (DSS) inspection.
5. The contractor may award subcontracts in furtherance of this effort. If access to classified information is required, the prime contractor is responsible to ensure compliance by the subcontractor for all security requirements. Copies of all subcontractor DD Forms 254 shall be forwarded to the Contracting Officer and the PEO STRI Security Office at the address listed in block 16d.
6. No security classification guide exists which is directly applicable to this effort. If, during this effort, it becomes necessary to create classified documentation for which there is no clear classification authority, the contractor shall notify the contract monitor, who will seek the assistance and appropriate guidance from the PEO STRI Security Office.
7. The contractor shall comply with security procedures in effect at government sites visited, and where contract work takes place. Contractor work will take place at

The services to be performed herein shall be performed primarily at PEO STRI, Orlando FL. Other places of performance include but are not limited to;

Ft. Benning, Georgia  
Fort Bliss, Texas  
Fort Bragg, North Carolina  
Ft. Campbell, Kentucky  
Fort Carson, Colorado  
Fort Drum, New York  
Fort Hood, Texas  
Fort Huachuca, AZ

Ft. Irwin, CA  
Ft. Knox, Kentucky  
Fort Leavenworth, Kansas  
Fort Lewis, Washington  
Ft. Monroe, Virginia and the Greater Tidewater Area  
Fort Sill, Oklahoma  
Fort Riley, Kansas  
Fort Rucker, Alabama  
Fort Sam Houston, Texas  
Ft. Monmouth, New Jersey  
Ft. Polk, Louisiana  
ARCENT, Iraq/Kuwait  
Redstone Arsenal, Alabama  
JFCOM, Suffolk, Virginia

**ITEM 10:**

**Ref item 10.e(1):** The Commander, U.S. Army Intelligence and Security Command (INSCOM) has the exclusive security responsibility for SCI information released to the contractor or developed under this contract.

**Ref item 10.e(2):** Access to intelligence information, Ch. 9 (section 3), NISPOM, defines such information and identifies authorized markings. The control, established by such markings, and the policies and procedures given in para.12, DCID 1/7 (DoD 5230.22) are part of the security specifications for this contract.

**Ref Item 10.j:** Protect “For Official Use Only” information the same as company proprietary information and as specified in the NISPOM, Chapter 5, Section 5. Also see Attachment For Official Use Only (FOUO) for additional guidance.

**ITEM 11:**

**Ref item 11.a:** All classified services rendered in performance of this contract will be conducted at designated government approved facilities.

**Ref item 11.f:** This contract may require your company to have access to classified information in an overseas area. The specific overseas area(s) will be provided by the Contract Monitor or the Contracting Officer. Classified information or materials will remain under the direct control of the US government while in an overseas area unless prior approval is granted by this command. Release of classified information to a foreign entity will be accomplished in accordance with Chapter 10, NISPOM.

**Ref item 11.g:** The contractor is authorized to use the services of Defense Technical Information Center (DTIC) and is required to prepare and process a DD Forms 1540 and 2345 to registration for Scientific and Technical Information Services. The contracting activity must be involved in certifying need-to-know to DTIC.

**Attachment 1****“FOR OFFICIAL USE ONLY” ADDENDUM**

1. FOR OFFICIAL USE ONLY (FOUO) is not a security classification marking but it is used to identify official government sensitive controlled unclassified information that must be withheld from the general public under provisions of the Freedom of Information Act (FOIA).
2. The following procedures will be used to protect FOR OFFICIAL USE ONLY (FOUO) Information:

**HANDLING:** Access to FOUO material shall be limited to those employees who need the information in the performance of the contract.

**MARKING:** Any FOUO material released to a contractor must have the following statement on the cover of the first page; contact the user agency if it does not:

**This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the Freedom of Information Act (FOIA). Exemptions \_\_\_\_\_ apply.**

Any document containing FOUO information will be marked “For Official Use Only” at the bottom of the cover or first page and on each page containing FOUO information and on the reverse of the back cover or last page. No portion or paragraph marking will be shown.

If the FOUO information is within a classified document, an individual page containing classified and FOUO material will be marked at the top and bottom with the highest security classification of the page contents only. The FOUO marking will be placed at the bottom of those pages that contain only FOUO material and no classified material.

Mark other records or media such as computer printouts, photographs, tapes or graphics “For Official Use Only” in such a manner to ensure that the receiver or viewer knows that the product contains FOUO.

**STORAGE:** During working hours, FOUO information shall be protected in such a manner to preclude other personnel in the same area who do not have a need for the information from having access to or viewing it. During non-working hours, the FOUO information shall be stored in such a manner to preclude unauthorized access. If internal building security is provided, the FOUO information may be stored in unlocked files or desks. If internal building security is not provided, the material must be protected by locked buildings or rooms, or the material may be stored in locked receptacles such as file cabinets, bookcases or desks. There is no requirement to purchase security containers adequate for storage of classified material to store FOUO information.

**TRANSMISSION:** FOUO information may be transmitted by regular U.S. Postal Service mail or U.S. commercial express mail services authorized for unclassified material. The transmission of FOUO material by regular telephone or internet is discouraged unless absolutely necessary in the performance of the contract and is time sensitive. FOUO material will not be placed on the World Wide Web that is accessible to the general public. FOUO information may be transmitted over telephone lines in digital form such as fax machines or telecopiers.

**UNAUTHORIZED DISCLOSURE:** The unauthorized disclosure of FOUO information does not constitute a security violation; however, the originator or User Agency will be informed of the disclosure. The unauthorized disclosure of FOUO information that is protected by the Privacy Act may result in criminal sanctions under that statute. Additional guidance is available from the PEO STRI Security Office.