

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED <p style="text-align: center;">TOP SECRET</p> b. LEVEL OF SAFEGUARDING REQUIRED <p style="text-align: center;">NONE</p>																																																																																						
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		<input checked="" type="checkbox"/>		a. ORIGINAL <i>(Complete date in all cases)</i>		DATE (YYYYMMDD) 20101229																																																																																				
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO.	DATE (YYYYMMDD)																																																																																				
<input checked="" type="checkbox"/> c. SOLICITATION OR OTHER NUMBER HC1028-11-R-2010		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>		DATE (YYYYMMDD)																																																																																				
4. IS THIS A FOLLOW-ON CONTRACT? <input checked="" type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ (See Block-13) _____ (Preceding Contract Number) is transferred to this follow-on contract.																																																																																										
5. IS THIS A FINAL DD FORM 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 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. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
THIS DD254 IS FOR SOLICITATION PURPOSES ONLY. A PRIME CONTRACT DD254 WILL BE PROVIDED UPON CONTRACT AWARD.																																																																																										
7. SUBCONTRACTOR																																																																																										
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
TBD																																																																																										
8. ACTUAL PERFORMANCE																																																																																										
a. LOCATION			b. CAGE CODE		c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>																																																																																					
See Block 13.																																																																																										
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Non-personal services for scientific, engineering, technical and administrative support for the Joint Interoperability Test Command, Fort Huachuca, AZ; Indian Head, MD; Falls Church, VA, and other locations authorized by the Contracting Officer (KO) and/or the Contracting Officer Representative (COR) .																																																																																										
<table border="1" style="width:100%; border-collapse: collapse;"> <thead> <tr> <th style="width:35%;">10. CONTRACTOR WILL REQUIRE ACCESS TO:</th> <th style="width:5%;">YES</th> <th style="width:5%;">NO</th> <th style="width:35%;">11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</th> <th style="width:5%;">YES</th> <th style="width:5%;">NO</th> </tr> </thead> <tbody> <tr> <td>a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>b. RESTRICTED DATA</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>b. RECEIVE CLASSIFIED DOCUMENTS ONLY</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>c. RECEIVE AND GENERATE CLASSIFIED MATERIAL</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>d. FORMERLY RESTRICTED DATA</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>e. INTELLIGENCE INFORMATION</td> <td></td> <td style="background-color: #cccccc;"></td> <td>e. PERFORM SERVICES ONLY</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>(1) Sensitive Compartmented Information (SCI)</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>(2) Non-SCI</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>f. SPECIAL ACCESS INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>h. REQUIRE A COMSEC ACCOUNT</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>g. NATO INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>i. HAVE TEMPEST REQUIREMENTS</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>h. FOREIGN GOVERNMENT INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>i. LIMITED DISSEMINATION INFORMATION</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td>k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE</td> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>j. FOR OFFICIAL USE ONLY INFORMATION</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>l. OTHER <i>(Specify)</i></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>k. OTHER <i>(Specify)</i> NC2-ESI Class D Restricted Area</td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td></td> <td>Provide Visit Requests. IT-I and IT-II access required.</td> <td></td> <td></td> </tr> </tbody> </table>							10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO	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> NC2-ESI Class D Restricted Area	<input checked="" type="checkbox"/>		Provide Visit Requests. IT-I and IT-II access required.		
10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO																																																																																					
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> NC2-ESI Class D Restricted Area	<input checked="" type="checkbox"/>		Provide Visit Requests. IT-I and IT-II access required.																																																																																							

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*)

Contracting Officer, DISA/DITCO PL8315, P.O. 12798, Fort Huachuca, AZ 85670-2798 and DISA Public Affairs Office (PAO), and, for Congressional congressional, the DISA Congressional Affairs (CA) office. Public release of SCI/SAP material is not authorized.

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.*)

This DD Form 254 reflects the security requirements for the contract when awarded. Pre-award access is not required.

a. Reference Item 4.

Classified material received or generated under NBCHC020001, NBCHC020002, or NBCHC020003 is transferred to this follow-on contract.

b. Reference Item 8a:

Contract Performance is restricted to the Joint Interoperability Test Command, Fort Huachuca, AZ; Indian Head, MD; Falls Church, VA, and other locations authorized by the Contracting Officer (KO) and/or Contracting Officer Representative (COR).

c. Reference Item 10a:

Contractor is authorized to receive Government furnished cryptographic equipment. Access to classified COMSEC information requires a final U.S. Government clearance at appropriate level. Further disclosure of COMSEC information by contractor, to include subcontracting, requires prior approval of the government contracting activity. Non-accountable COMSEC information, though not tracked in the COMSEC material control system, may still require a level or control within a document control system. Refer to NSA/CSS Manual 3-16, Control of COMSEC Material, page E-4 for guidance.

d. Reference Item 10c:

This contractor is permitted access to CNWDI in performance of the contract. The Government program manager or designated representative ensures the contractor Facility Security Officer (FSO) is briefed for access to CNWDI by a Government representative prior to granting access.

BLOCK-13 CONTINUED ON SEPARATE PAGES.

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.*)

The contractor will be provided and will abide by DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems", 5 Jun 99 and by DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)," 18 Nov 02. Provided under separate cover. OPSEC requirements apply and guidance provided in block 13 as reference item 11j.


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.*)

The DISA Security Division (MPS6) is responsible for inspection of SCI under this contract. The cognizant Special Access Program (SAP) Management Office is responsible for inspection of all SAP related information under this contract. DSS is relieved of inspection authority.

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 JOSE MUNOZ	b. TITLE Contracting Officer's Industrial Security Rep	c. TELEPHONE (<i>Include Area Code</i>) (520)538-5573
--	---	--

d. ADDRESS (*Include Zip Code*)
 JITC-JT2C, Attn: Security
 P.O. Box 12798
 Fort Huachuca, AZ 85670-2798

e. SIGNATURE


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

Item 13. SECURITY GUIDANCE (Continued)

e. Reference Item 10e(1):

This contract requires access to Sensitive Compartmented Information (SCI).

(a) The number of personnel required to access SCI is determined by the Contracting Officer Representative (COR)/ Task Monitor (TM) and DISA Special Security Office (SSO).

(b) The Director, Defense Intelligence Agency (DIA) and Director, Defense Information Systems Agency (DISA), as the executive agent for DIA, have exclusive security responsibility for SCI released to the contractor or developed under this contract.

(c) Contractor generated or Government furnished material may not be provided to the Defense Technical Information Center (DTIC). Contract generated technical reports will bear the statement '**Not Releasable to the DTIC per DoD Instruction 5230.24.**'

(d) All contractor personnel requiring access to SCI information must: be U.S. citizens, have been granted a final Director Central Intelligence Directive (DCID) 6/4 eligibility/security clearance by the U.S. Government, and have been indoctrinated for the applicable compartments of SCI access prior to being given any access to such information released or generated under this contract.

(e) Classified material released or generated under this contract is not releasable to foreign nationals without the expressed written permission of the Director (through the DISA SSO) and Director, DIA.

(f) SCI received under this contract may not be released to subcontractors without permission of the DISA SSO.

(g) The contractor and COR/TM will revalidate all SCI billets under this contract with the DISA SSO annually or when a revised DD Form 254 issued, whichever is sooner.

(h) All SCI visit requests by contractors shall be forwarded to the COR/TM for approval and need-to-know certification before being sent through the DISA SSO to the facility to be visited.

(i) All contractor SCI work and access will be at a designated government SCI Facility (SCIF).

f. Reference Item 10e(2).

The contractor will abide by DCID 6/6 (formerly 1/7), Security Controls on the Dissemination of Intelligence Information, 11 July 2001. Provided under separate cover.

g. Reference Item 10f:

(1) To execute this contract, additional security requirements in addition to DoD 5220.22-M will be required. The contractor shall comply with the security provisions of these programs. Marking and/or classification guidance for material originated or generated under this contract will be provided through the Special Access Program (SAP) Management Office under separate cover. Any material

Item 13. SECURITY GUIDANCE (Continued)

generated by the contractor (including drawings, correspondence, models, mockups, photographs, schematics, progress, special and inspection reports, engineering notes, computations and training aids) shall be classified according to content. Guidance for classification shall be derived from the applicable Security Classification Guides, documents, or special instructions. Such material shall not contain contractor logos or similar identifiers which identify the specific contractor or team members.

(2) The Contractor Special Security Officers shall coordinate through JITC Security Office with the DISA Security Office (MPS6) and SAP Management Office prior to subcontracting any portion of this contract.

(3) All personnel requiring access to SAP information must be U.S. citizens, have been granted a final U.S. Government security clearance, and have been indoctrinated for the applicable SAP prior to being given access to such information generated or received under this contract.

(4) Contractor generated or Government furnished material may not be provided to the DTIC. Contractor products will bear the statement: "Not Releasable to the DTIC" per DoDI 5230.24.

(5) Upon expiration of this contract, the contractor is required to have a close-out inspection by the DISA SSO and/or SAP Management Office to ensure disposition of material and equipment. The contractor shall request disposition instructions for all classified and unclassified project material. The contractor may be directed to properly destroy the material or return it. If classified/unclassified project material is to be retained by the contractor, every effort should be taken to transfer it to a follow-on contract or similar effort, if applicable. This must be done, however, with the Contracting Officer's (KO) approval. The material shall be returned or destroyed as instructed, unless written authorization by the KO to retain specific material for a specific period of time is received. Any exception to security policy shall be referred to the Cognizant Security Office and the DISA Security Office (MPS6) for coordination with the appropriate agency(s) and the KO.

h. Reference Items 10f and 11c:

This contract will be performed in a facility approved through JITC Security, DISA Security Office (MPS6) and/or the SAP Management Office in accordance with applicable SAP security requirements. The Defense Security Service (DSS) is relieved of security cognizance by the SAP Management Office, which will have responsibility for all SAP material and/or information released under this contract.

i. Reference Item 10g:

(1) Access to NATO requires a final U.S. Government security clearance at the appropriate level. A representative of the Government will brief the Facility Security Officer (FSO), who in turn will brief other contractor personnel requiring access under the contract. FSO will provide an updated Visit Authorization Request (VAR) for any personnel briefed NATO.

(2) Access up to and including NATO COSMIC material will be required for reference only at the User Agency sites and other government/contractor facilities authorized by the COR and/or the KO.

Item 13. SECURITY GUIDANCE (Continued)

j. Reference Item 10h:

Access to classified foreign government information requires a final U.S. Government clearance.

k. Reference Item 10j:

For Official Use Only (FOUO) Information. Contractor will be provided with and will abide by DoD Regulation 5400.7, DoD Freedom of Information Act Program, and DoD Regulation 5200.1-R, Information Security Program, Appendix-3. Guidance provided under separate cover.

l. Reference Item 10k (Other):

(1) This contract requires that specified contractor employees be granted access to Nuclear Command and Control - Extremely Sensitive Information (NC2-ESI). Employees requiring NC2-ESI access will be processed as follows:

(a) The DISA COR/TM will forward to the DISA NC2-ESI Coordinator (MPS6) through the JTC Security Office, via an Interoffice Memorandum, a request to process certain employees of the company for NC2-ESI access. The request will be marked with the appropriate markings (i.e., FOUO, Privacy Act Protected, etc.) and/or classification as may be required per the security classification guide. This request will contain the following for each individual:

- (1) Name and Social Security Number of the employee.
- (2) Company name, address, CAGE code, telephone number.
- (3) Date and place of birth for employee.
- (4) Citizenship of employee.
- (5) Citizenship of employee's spouse.
- (6) NC2-ESI Category required.
- (7) Employee's clearance level and date, investigation type and date.
- (8) Inclusive dates NC2 access will be required.
- (9) Contract number.
- (10) Contract expiration date.
- (11) Contract review date.
- (12) Justification for requesting NC2-ESI accesses (include referring Joint Chiefs of Staff (JCS) office or JCS POC).

Item 13. SECURITY GUIDANCE (Continued)

(b) The DISA NC2-ESI Coordinator (MPS6) prepares a memorandum, which includes a temporary access roster, justification from the government security official, and a copy(s) of the security clearance records from the Joint Adjudication Personnel System (JPAS). This memorandum will be forwarded to the approval authority (JCS).

(c) When temporary access to NC2-ESI has been approved by the JCS, the DISA NC2-ESI Coordinator (MPS6) will forward this information to the JITC Security Office and authorize the employee(s) to be briefed for access.

(d) The Contractor Facility Security Officer (FSO) is responsible for notifying the DISA NC2-ESI Coordinator (MPS6) through the JITC Security Office when the employee is transferred from one facility to another within the company, when the employee's employment is terminated, when they resign, or have been transferred and do not require continued access.

(e) The Facility Security Officer (FSO) is responsible for ensuring that the employees complete the required security forms for submission to DSS Facility Security Branch in a timely manner.

(f) Information that an individual has been granted access to NC2-ESI is unclassified information.

(2) This contract requires access to DISA Controlled Access Areas (CAA) in accordance with DISA Instruction 240-110-33, Physical Security.

(a) The JITC Compound and all buildings designated as JITC space are classified as CAAs. Personnel designated to work in JITC spaces shall obtain and maintain eligibility for access to a minimum of SECRET information.

(b) New employees will be given 90 days to receive at a minimum interim eligibility for access to SECRET information. If eligibility is not received, a waiver may be granted by the JITC Commander with final approval of the Contracting Officer on a case-by-case basis.

(c) Contractor personnel who do not have a security clearance due to revocation, denial or withdrawal will not be eligible to work on this DISA contract whether as a prime or sub contractor. The Contracting Officer will issue notice to the contractor of any security eligibility violations and denial of an employee's ability to work under the contract.

(d) All contractors must be able to obtain and maintain eligibility for IT access. The minimum IT level access required for all contractor employees will be IT-II.

(e) All classified information processed under this contract is the property of the U.S. Government.

(1) Detailed Security Classification Guides will be provided under separate cover.

(2) The COR must be notified and approve the receipt and/or generation of classified information under this contract.

Item 13. SECURITY GUIDANCE (Continued)

(3) The contractor will be required to prepare an Automated Information System Standard Practice Procedure (AIS/SPP) for their classified AIS operations and the system will require approval of the CSO/CSA in accordance with NISPOM, Chapter 8.

(4) Upon contract termination/expiration, the U.S. Government will be contacted for disposition.

(3) Due to access eligibility requirements of this contract the following additional training is required by contractors requiring access to classified information. The contractor is responsible for completing DOD, DISA, JITC and local post mandated training requirements in performance of the contract. The JITC training office provides access to all training sources and contractors are encouraged to attend/make use of the training opportunities provided. The contractor Training Coordinator, Facility Security Officer, or designated representative is responsible to ensure employees meet these training requirements.

(a) Standard Operating Procedure (SOP) review annually.

(b) Derivative Classification (DSS Course IF103.16) - Prerequisite for access to classified information systems.

(c) Marking Classified Documents (DSS Course IF105.16) – Prerequisite for access to classified information systems.

m. Reference Item 11a:

(1) Contract performance is restricted to locations listed in Block 9. The using contractor or Government activity will provide security classification guidance for the performance of this contract.

(2) The COR must be notified and approve the receipt and/or generation of classified information under this contract.

(3) All classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Upon completion or termination of this contract, the COR will be contacted for destruction or disposition instructions.

n. Reference Item 11f:

Contractors when performing or traveling outside the United States under this contract will:

(a) All personnel will obtain an Area of Responsibility (AOR) specific foreign travel brief within 90 days of travel and will provide proof of training to the COR/TM.

(b) All personnel will receive the Antiterrorism Level I Awareness training within one year prior to travel.

o. Reference Item 11g:

(1) Technical information on file at the Defense Technical Information Center will be made available to the contractor if the contractor requires such information.

Item 13. SECURITY GUIDANCE (Continued)

(2) The contractor must prepare and forward a DD Form 1540 to the COR/TM for authorization BEFORE the services may be requested.

p. Reference Item 11j:

(1) The contractor will comply with special Operations Security (OPSEC) requirements contained in DoD Directive 5205.2, DoD OPSEC Program, DISA OPSEC.

(2) OPSEC applies to the SAP portions of this contract and will be conducted in accordance with DoD 5220.22-M Sup-1 and as described in applicable Security Classification Guides. Specifically, an OPSEC orientation must be provided to newly assigned personnel in concert with the SAP Indoctrination. OPSEC will also be covered in annual refresher training. These briefings will be held at appropriate SAP locations.

q. Reference Item 11i:

(1) The COR must certify contractor employee's need for access to JITC activities by signing employee's Visit Authorization Request (VAR). Employee VARs cannot exceed one year or the length of the contract whichever is shorter. VAR content: Company Name, Address, Cage Code, Contract Number, Facility Security Officer (FSO)'s Name/Phone/Signature, employee identification data (SSN, Name, DoB, PoB, citizenship), clearance data (clearance level, clearance date, granting agency, investigation type, investigation date, investigation agency).

VARs for access to JITC activities will be addressed to:

(a) Fort Huachuca:

Commander, Joint Interoperability Test Command
P.O. Box 12798
Fort Huachuca, AZ 85670-2798.

(b) Indian Head:

Commander, Joint Interoperability Test Command
Indian Head Div, NSWC
101 Strauss Avenue, Bldg 900
Indian Head, MD 20640-5035.

(2) The COR/TM must be notified and approve the receipt and/or generation of classified information under this contract. All classified information received and/or generated under this contract is the property of the U.S. Government regardless of proprietary claims. Upon completion or termination of this contract, the U.S. Government will be contacted for destruction or disposition instructions.

(3) Estimated date of completion for this contract is TBD .

THIS DD FORM 254 INCLUDES NO ATTACHMENTS.