

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
<i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)</i>				a. FACILITY CLEARANCE REQUIRED Secret	
				b. LEVEL OF SAFEGUARDING REQUIRED N/A	
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 (YYMMDD) 3 12 19
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>	Revision No. Date (YYMMDD)
<input checked="" type="checkbox"/> c. SOLICITATION OR OTHER NUMBER FA8726-04-R-0002		DUE Date (YYMMDD) 4 03 11		c. FINAL <i>(Complete Item 5 in all cases)</i> Date (YYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <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					
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 requested dated _____, retention of the identified 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 TBD		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE TBD		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
8. ACTUAL PERFORMANCE					
a. LOCATION TBD		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT Theater Deployable Communications Modules and Kits. Integrate and deliver suites of communications equipment for deployed Air Force operations.					
10. THIS CONTRACT WILL REQUIRE ACCESS			11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		
YES NO			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 type="checkbox"/>			b. RECEIVE CLASSIFIED DOCUMENTS ONLY <input checked="" type="checkbox"/>		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION <input type="checkbox"/>			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL <input checked="" type="checkbox"/>		
d. FORMERLY RESTRICTED DATA <input type="checkbox"/>			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE <input checked="" type="checkbox"/>		
e. INTELLIGENCE INFORMATION <input type="checkbox"/>			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 type="checkbox"/>			h. REQUIRE A COMSEC ACCOUNT <input checked="" type="checkbox"/>		
g. NATO INFORMATION <input type="checkbox"/>			i. HAVE TEMPEST REQUIREMENTS <input checked="" type="checkbox"/>		
h. FOREIGN GOVERNMENT INFORMATION <input type="checkbox"/>			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS <input checked="" type="checkbox"/>		
i. LIMITED DISSEMINATION INFORMATION <input 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>		
k. OTHER <i>(Specify)</i> <input checked="" type="checkbox"/>					

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 Government authority. Proposed public releases shall be submitted for approval prior to release

Direct Through (Specify):

HQ ESC/PA
9 Eglin Street
Hanscom AFB, MA 01731-2118

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 need 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/guidelines/extracts reference herein. Add additional pages as needed to provide complete guidance.)

The National Industrial Security Program Operating Manual (NISPOM), January 1995, applies to this contract.

The Program Manager is Joan Wandrei, 5 Eglin Street, Hanscom AFB, MA 01731-2100.

The expiration date of the contract is TBD.

Ref Blk 10a: See Atch 1 (COMSEC)

Ref Blk 10j: See Atch 2 (FOUO)

Ref Blk 11a: Releasing contractor will furnish complete classification guidance for services to be performed. Performance is restricted to TDC contractor and TDC user locations.

Coordination: ESC/INP Kellie A. O'Brien 2/25/04

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

Yes No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

Yes No

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.

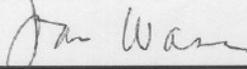
a. TYPED NAME OF CERTIFYING OFFICIAL
JOAN WANDREI

b. TITLE
Theater Deployable Communications Program
Manager

c. TELEPHONE (Include Area Code)
781-377-7965

d. ADDRESS (Include Zip Code)
ESC/NI4T
5 Eglin Street
Hanscom AFB, MA 01731-2100

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. ADMINISTRATION CONTRACTING OFFICER
- f. OTHERS AS NECESSARY

ATTACHMENT 1
Communications Security (COMSEC)

The National Security Agency Industrial COMSEC Manual (NSA Manual 90-1), shall apply to this contract. Access to classified COMSEC information shall be restricted to U.S. Citizens who: have been granted a final government security clearance; have a valid need-to-know (as defined in the National Industrial Security Program Operating Manual (NISPOM)); and have successfully completed a non-lifestyle, counterintelligence scope polygraph examination if required, administered in accordance with DoD or agency requirements and applicable laws. Non-U. S. Citizens, including immigrant aliens, are not eligible for access to classified COMSEC material or information. Access to unclassified, Controlled Cryptographic Items (CCI) will be limited to U. S. Citizens requiring such access. Within the U. S., Non-U.S. Citizens may perform building maintenance or custodial duties in contractor spaces containing installed CCI equipment, provided that equipment is not keyed. For access to certain types of COMSEC information, a CRYPTO access or COMSEC briefing may be required. Refer to Section II, paragraph 9, of NSA Manual 90-1 for briefings required under specific types of access. The Facility Security Officer (FSO) must provide a current listing of all individuals granted cryptographic access for each contract or Memorandum of Agreement (MOA) to the appropriate government Program Office.

ATTACHMENT 2
FOR OFFICIAL USE ONLY INFORMATION

1. FOR OFFICIAL USE ONLY INFORMATION:

a. The “For Official Use Only” (FOUO) marking is assigned to information at the time of its creation by 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 (FOIA).

b. 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 or portions of it.

2. IDENTIFICATION 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 markings 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 of information appearing on the page. If an individual portion contains FOUO information but no classified information, the portion will be marked, “FOUO.”

c. Any FOUO information released to a contractor by a 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 FOUO marking can only be accomplished by the originator or other competent authority. When the FOUO status is terminated, all known holders will be notified to the extent practical.

3. DISSEMINATION: Contractors may disseminate FOUO information to their employees and subcontractors who have a need for the information in connection with a classified contract.

4. STORAGE: During working hours, FOUO 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.

5. TRANSMISSION: FOUO information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth class mail.

6. DISPOSITION & DISCLOSURE: When no longer needed, FOUO information may be disposed of by tearing each copy into pieces to preclude reconstructing, and placing it in a regular trash container. Unauthorized disclosure of FOUO 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.