

<b>DEPARTMENT OF DEFENSE</b>				<b>1. CLEARANCE AND SAFEGUARDING</b>		
<b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b>				a. FACILITY CLEARANCE REQUIRED		
<i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				<b>SECRET</b>		
				b. LEVEL OF SAFEGUARDING REQUIRED		
				<b>SECRET</b>		
<b>2. THIS SPECIFICATION IS FOR: (X and complete as applicable)</b>			<b>3. THIS SPECIFICATION IS: (X and complete as applicable)</b>			
	a. PRIME CONTRACT NUMBER		a. ORIGINAL (Complete date in all cases)	DATE (YYMMDD)		
	b. SUBCONTRACT NUMBER		b. REVISED (Supersedes all previous specs)	Revision No.	DATE (YYMMDD)	
<b>X</b>	c. SOLICITATION OR OTHER NUMBER DAAA09-01-R-0068	DUE DATE (YYMMDD) 01 06 04	c. FINAL (Complete item 5 in all cases)		DATE (YYMMDD)	
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 <u>DAAB07-97-D-C759</u> (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 identified classified material is authorized for the period of _____						
<b>6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)</b>						
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
<b>7. SUBCONTRACTOR</b>						
a. NAME, ADDRESS, AND ZIP CODE		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
<b>8. ACTUAL PERFORMANCE</b>						
a. LOCATION		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)			
<b>9. GENERAL IDENTIFICATION OF THIS PROCUREMENT</b>						
LOGISTICS CIVIL AUGMENTATION PROGRAM (LOGCAP) SUPPORT CONTRACT						
<b>10. THIS CONTRACT WILL REQUIRE ACCESS TO:</b>						
	YES	NO	<b>11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:</b>		YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<b>X</b>		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY			<b>X</b>
b. RESTRICTED DATA		<b>X</b>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY			<b>X</b>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		<b>X</b>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		<b>X</b>	
d. FORMERLY RESTRICTED DATA		<b>X</b>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE			<b>X</b>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY		<b>X</b>	
(1) Sensitive Compartmented Information (SCI)		<b>X</b>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		<b>X</b>	
(2) Non-SCI	<b>X</b>		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER			<b>X</b>
f. SPECIAL ACCESS INFORMATION		<b>X</b>	h. REQUIRE A COMSEC ACCOUNT		<b>X</b>	
g. NATO INFORMATION		<b>X</b>	i. HAVE TEMPEST REQUIREMENTS		<b>X</b>	
h. FOREIGN GOVERNMENT INFORMATION		<b>X</b>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		<b>X</b>	
i. LIMITED DISSEMINATION INFORMATION		<b>X</b>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<b>X</b>	
j. FOR OFFICIAL USE ONLY INFORMATION		<b>X</b>	l. OTHER (Specify)			
k. OTHER (Specify)		<b>X</b>				<b>X</b>

**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):

PM LOGCAP

5001 Eisenhower Avenue

Alexandria, VA 22333

DSN: 767-0428

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.)

A. The contractor will have access to SECRET-NOFORN information. All contractor's personnel having access to classified information, hardware, or software or unclassified software must be U.S. citizens with a final SECRET clearance issued by the Government.

B. Contractor will require custody of classified materials through SECRET.

C. (11C) Security Requirement Check List, see Appendage #1.

D. (11i) Equipment that electronically process or generate classified information will conform with compromising emanation control criteria, see Appendage #3, (Tempest).

E. Document receipts and/or retention requests should be provided to the Contracting Officer.

F. Discrepancies in classification or challenges to classification will be addressed to the activity listed in block 16d of this form.

G. (10j) FOUO will be handled IAW Appendage #4.

H. (10.e.(2)) Intelligence Materials Access Requirements, see Appendage #5.

I. Appendage #2, "Additional Security Requirements for COMSEC."

**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, explain and 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

JAMES F. FOLKS

b. TITLE

PROGRAM MANAGER

c. TELEPHONE (Include Area Code)

DSN 767-0428

703-617-0428

d. ADDRESS (Include Zip Code)

HQ US AMC

5001 Eisenhower Avenue, Attn: SOSFS-COL

Alexandria, VA 22333-0001

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

APPENDAGE 1  
(Page 1 of 4)

### SECURITY REQUIREMENTS CHECKLIST

Reference: 1. National Industrial Security Program Operating Manual (NISPOM)  
2. Cryptographic Supplement to National Industrial Security Program Operation Manual (NISPOM).

#### General Information

a. The designation as it appears in the classification columns on DD Form 254 indicated the highest classification of applicable contact items, and also signifies that these items shall be safeguarded, stored, accounted for, and transmitted or transferred within and without the contractor's facilities by contractors in accordance with the procedures specified in Reference 1.

b. As stated in a. above, the column markings indicate the highest classification included with the specified item; however, lower classifications may be assigned to individual items there under by the category criteria set forth in the following notes.

c. In those cases where doubt exists or where an item does not clearly fall into one of the listed categories, specific guidance as to its proper classification and method of handling shall be obtained from the Contracting Officer or his duly authorized technical representative(s).

NOTE 1 The following criteria apply to any design information, drawings or sketches, photographs, models, mock-ups, training aids, and manufacturing aids produced by the contractor.

a. Those items which reveal information about the cryptographic system under development (e.g.: cryptographic logic, cryptoalarm, permuting devices etc.) shall be classified SECRET and shall be handled by the contractor in accordance with the procedures specified in Reference 2.

b. Those items, which indicate non cryptographic details of the equipment and reveal specific information concerning related technical areas shall be classified CONFIDENTIAL and shall be handled by the contractor in accordance with the procedures in Reference 1.

c. Those items which reveal no cryptographic or related details but which deal with the functioning of the equipment (e.g.: certain individual mechanical parts, subassemblies, electrical or electronic circuit components, power supplies, mounting facilities and packaging techniques) shall be UNCLASSIFIED.

Appendage #1  
(page 2 of 4)

**SECURITY REQUIREMENTS CHECKLIST**

Note 2 The following criteria apply to any Specialized Manufacturing Techniques developed or used by the contractor.

a. Those specialized manufacturing techniques, which may reveal information concerning the cryptographic features of the end item under development shall be classified CONFIDENTIAL and shall be handled by the contractor in accordance with the procedures specified in Reference 2.

b. Those specialized manufacturing techniques, which reveal no information concerning the cryptographic features of the end item under development shall be UNCLASSIFIED.

NOTE 3 The following criteria apply to any status progress, technical or conference reports and administrative correspondence produced by the contractor.

a. Those technical reports (including status, progress and conference) which reveal details of the cryptographic system involved in this contract shall be classified SECRET and shall be handled by the contractor in accordance with the procedures specified in Reference 2.

b. Those technical reports (including status, progress, and conference) which do not reveal details of the cryptographic system involved but which do reveal related detailed functions of the equipment shall be classified CONFIDENTIAL and shall be handled by the contractor in accordance with the procedures as specified in Reference 1.

c. Those technical reports, conference reports and correspondence of a general administrative nature dealing with the contract, scheduling, and system delivery shall be UNCLASSIFIED.

NOTE 4 The following criteria apply to any tests conducted or test data produced by the contractor in the course of this development.

a. Those tests conducted and test data produced which may reveal details of the cryptographic system involved in this contract shall be classified SECRET and shall be handled by the contractor in accordance with the procedures specified in Reference 2.

b. Those tests conducted and test data developed which do not reveal details of the cryptographic system but which do reveal details of related technical areas involved in the end item under development shall be classified CONFIDENTIAL and shall be handled by the contractor in accordance with the procedures specified in Reference 1.

Appendage #1  
(Page 3 of 4)

**SECURITY REQUIREMENTS CHECKLIST**

c. Those tests conducted and test data developed, which relate to the general purpose, application or features of the end item under development (e.g.: reliability and environmental tests on specific subassemblies, mechanical or electronic components or the system) shall be UNCLASSIFIED.

NOTE 5

Any documents, drawings, items of equipment or components, which are supplied to the contractor, as Government Furnished Property will be appropriately classified by the originator. If such items reveal specific cryptographic information they will be transmitted by cryptographic channels, and shall be handled by the contractor in accordance with the procedures specified in Reference 2. If they do not reveal specific cryptographic information they will be transmitted by other authorized channels, and if classified, shall be handled by the contractor in accordance with the procedures specified in Reference 1.

NOTE 6

Classified COMSEC material released or generated under this contract is not releasable to Foreign Nationals without the express permission of the Director, NSA.

Note 7

Refer to Additional Security Guidelines for COMSEC, dated July 1996, attached as APPENDAGE #2 to the DD Form 254 for additional security requirements.



APPENDAGE #2 TO DD FORM 254

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Provided by Security Support Division  
Directorate for Intelligence and Information Security

## ADDITIONAL COMSEC GUIDELINES

Contractor Generated COMSEC Material: Any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs, and special inspection reports, engineering notes, computation, and training aids) will be classified according to its own content. Classification guidance will be taken from other elements of this contract Security Classification specification DD Form 254, Government furnished equipment or data, or special instructions issued by the contracting Officer, of his/her duty appointed representative.

## REQUIREMENTS

## REQUIREMENTS:

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
2. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement, "Not releasable to the Defense Technical Information Center per DoD Directive 5100-38".
3. No contractor generated COMSEC or government furnished material may be provided to the Defense Documentation Center. Contractor generated technical reports will bear the statement, "Not releasable to the Defense Documentation Center per DoD Instruction 5100-28".
4. Classified paper COMSEC material may be destroyed by burning, pulping, or pulverizing. When a method other than burning is used, all residue must be reduced to pieces 5mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
5. The following downgrading and declassification notation applies to all classified COMSEC information provided to and generated by the contractor:  
CLASSIFIED BY: NSA/CSSM-123-2  
DECLASSIFY ON: Source marked "OADR" Originating Agency Determination Required  
DATE OF SOURCE: (Date of document from which information is derived)
6. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel

holding a contractor generated CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the Director, NSA. If applicable, contractor personnel having access to TOP SECRET COMSEC material must comply with AR-380-40, Chapter 8, and be registered in the Department of the Army Cryptographic Access Program (DACP).

7. Unclassified COMSEC information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information is strictly prohibited.

8. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.

9. The requirements of the DoD 5220-22-M National Industrial Security Program Operation Manual (NISPOM) and COMSEC Supplements are applicable to this effort.

10. Additional notices are to be affixed to the cover and title or first page of contractor generated COMSEC documents:

a. "COMSEC MATERIAL-ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE".

B. THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONAL WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA".

## APPENDAGE #3 TO DD FORM 254

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Provided by Security Support Division  
Directorate for Intelligence and Information Security

1. Reference: DoD 5220-22-M, National Industrial Security Program Operating Manual.
2. In accordance with guidance referenced above, TEMPEST Countermeasures will only be employed where a threat of exploitation exists. A TEMPEST assessment must be performed by the contractor and be validated by INSCOM TEMPEST elements prior to allocation of army funds for TEMPEST countermeasures.
3. When electronic equipment is used to process classified information, a written TEMPEST/Risk Analysis will be provided to the contracting officer, or designated representatives (Command Tempest Control Officer, AMSEL-MI-CI-A), only if either of the following conditions apply:
  - a. The contractor will use electronic equipment/facilities to process TOP SECRET, SCI, SAP, SIOP, Restricted Data information; or
  - b. The contractor does not maintain complete physical access control of the facility, e.g., the contractor is located in a suite.
4. Complete TEMPEST assessments will be protected at a minimum of "FOR OFFICIAL USE ONLY". A classification is warranted if classified threat information on the facility is included or significant vulnerabilities are identified.

APPENDAGE #4 TO DD FORM 254

(Page 1 of 2)

**SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION**

Provided by Security support Division  
Directorate for Intelligence & Information Security

1. The "For Official Use Only" (FOUO) 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 it is used on official government information that maybe 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 instruction received from 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 information or portions of it.

4. 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 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 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 "FOR OFFICIAL USE ONLY" marking can only be accomplished by the originator or other competent authority. When "FOR OFFICIAL USE ONLY" status is terminated, all known holders will be notified to the extent practical.

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

APPENDAGE #4 TO DD FORM 254  
(Page 2 of 2)

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 building 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 by forth-class mail.

8. DISPOSITION: 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 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.

APPENDAGE 5 TO DD FORM 254

**INTELLIGENCE MATERIALS ACCESS REQUIREMENTS**

Provided by Security Support Division  
Directorate for Intelligence & Information Security

No Intelligence materials are to be provided in support of the contract without the prior approval of the Acquisition & Technology Support Division (ATSD), Directorate for Intelligence and Information Security (DIIS), U.S. Army Communications-Electronics Command (USACECOM). Any intelligence materials so provided will be disseminated solely by the ATSD, and will be accompanied by both a Letter of Instruction governing control of the materials provided, and a Letter of Transmittal, identifying the materials loaned and the duration of the loan. This service only pertains to elements supported by the Acquisition & Technology Support Division, DIIS, and USACECOM.