

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION				1. CLEARANCE AND SAFEGUARDING	
<i>(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)</i>				a. FACILITY CLEARANCE REQUIRED Top Secret	
				b. LEVEL OF SAFEGUARDING REQUIRED Top Secret	
2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			3. THIS SPECIFICATION IS: (X and complete as applicable)		
<input type="checkbox"/>	a. PRIME CONTRACT NUMBER		X	a. ORIGINAL (Complete date in all cases)	Date (YYMMDD) 031216
<input type="checkbox"/>	b. SUBCONTRACT NUMBER		<input type="checkbox"/>	b. REVISED (Supersedes all previous specs)	Revision No. Date (YYMMDD)
X	c. SOLICITATION OR OTHER NUMBER F19628-03-R-0062	Due Date (YYMMDD) TBD	<input type="checkbox"/>	c. FINAL (Complete Item 5 in all cases)	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 _____ (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 _____.					
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)					
a. NAME, ADDRESS, AND ZIP CODE TBD		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE TBD		b. CAGE CODE		c. COGNIZANT SECURITY OFFICES (Name, Address, and Zip Code)	
8. ACTUAL PERFORMANCE					
a. LOCATION TBD		b. CAGE CODE		c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT GROUND ELEMENT MEECN SYSTEM (GEMS), Software and Hardware development, production, and test.					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>	X
b. RESTRICTED DATA	X	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	X	<input type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA:	X	<input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	<input type="checkbox"/>	X
(1) Sensitive Compartmented Information (SCI)	X	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	X	<input type="checkbox"/>
(2) Non-SCI	<input type="checkbox"/>	X	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	X	h. REQUIRE A COMSEC ACCOUNT	X	<input type="checkbox"/>
g. NATO INFORMATION	X	<input type="checkbox"/>	i. HAVE A TEMPEST REQUIREMENT	X	<input type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	X	<input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	<input type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	X	<input type="checkbox"/>	l. OTHER (Specify).	X	<input type="checkbox"/>
k. OTHER (Specify) Access to SIOP, SCI and NOFORN information will be required.	X	<input type="checkbox"/>	Notification of Government Security activity applies. AF FARm52.204-9000		

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 release shall be submitted for approval prior to release

Direct

Through (Specify):

ESC/PA, 9 Eglin Street, Hanscom AFB, MA. 01731-5000. No public release of SCI is authorized. (SCI addendum attachment 1)

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 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 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 document/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.

13B. ESC/ND Security Specialist coordination:

13E. The GEMS Program Manager is:

/// signed /// Date: 25 Feb 2004
Mr. Mark Hutton
ESC/ND
11 Eglin Street
Hanscom AFB, MA 01731-2120
DSN: 478-2683 Comm.: (781) 377-2683

/// signed /// Date: 25 Feb 2004
David C. Walker, Capt, USAF
ESC/NDM
11 Eglin Street
Hanscom AFB, MA 01731-2120
DSN: 478-8903 Comm.: (781) 377-8903

13F. The GEMS contract monitor is:

13G. ESC/NI60, Hanscom AFB, EMSEC Manager coordination:

/// signed /// Date: 25 Feb 2004
Ms. Kathy Viano
ESC/NDK
11 Eglin Street
Hanscom AFB, MA 01731-2120
DSN 478-7746 Comm. 781-377-7746

/// signed /// Date: 25 Feb 2004
Mr. Alfred Knoll
ESC/NI60
50 Hamilton Street
Hanscom AFB, MA 01731-1621
DSN 478-4716 Comm. 781-377-4716

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

SCI requirements apply. See attachment 1.
FOUO applies, See attachment 2.
Special EMSEC (TEMPEST) requirements apply. See attachment 3.
General Intelligence Material/Foreign Disclosure applies. See Attachment 4

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

See attachments.

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 Capt. David C. Walker	b. TITLE GEMS Program Manager Strategic Command & Control SPO	c. TELEPHONE (Include Area Code) (781) 377-8903
---	---	--

d. ADDRESS (Include ZIP Code)
ESC/NDM
11 Eglin Street
Hanscom AFB, MA 01731-2120

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

GEMS Program DD Form 254, Continuation Sheet

Ref Item 8. Actual performance: Some work will take place at Hanscom AFB MA and the GEMS site locations mentioned in the program documentation. Contractor personnel performing under this contract will not have accountability for classified information or material at these locations.

Ref Item 10a. 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.

Ref Item 10c. Contractor personnel with a final US Government clearance must be CNWDI briefed prior to access. CNWDI is not releasable to contractor employees who have been granted a reciprocal clearance.

Ref Item 10e.(1) Access to SCI materials will be required to permit access to Command Centers and Command Center. See Attachment 1.

Ref Item 10e.(2) General Intelligence Material/Foreign Disclosure applies. See Addendum, Atch. 4.

Ref Item 10g Access to NATO SECRET will be required.

Ref Item 10j FOUO Applies. See Addendum, Atch 2.

Ref Item 10k. Other - Access to SIOP information will be required.

Ref Item 11c Any classified information generated in the performance of this contract shall require the contractor to either apply derivative classification and markings consistent with the source material, or be governed by the following Security Classification Guide(s).

1. Chairman of the Joint Chiefs of Staff Emergency Action Procedures, Volume I, Security Classification
2. National Military Command System (NMCS) Security Classification Guide

Ref Item 11.d The contractor is required to provide adequate and approved storage for classified hardware and material to the level of TOP SECRET, which because of size or quantity cannot be safeguarded in an approved storage container.

Ref Item 11f Overseas contractor performance will occur at those GEMS site locations listed in the program documentation.

Ref Item 11. g Special Access Required (SAR) and Intelligence material is not releasable to DTIC.

Ref Item 11i. EMSEC Requirements apply. See Addendum Atch 3.

Ref Item 11j OPSEC Requirements Apply. See Chairman of the Joint Chiefs of Staff Emergency Action Procedures, Volume I, Security Classification.

Ref Item 11 k DCS address is HQ Defense Courier System, Building P-830, Ft George Meade, 20755-5370

Ref Item 13a. Servicing Security Activity at Hanscom AFB, is ESC/INP, 102 Barksdale St., Hanscom AFB, MA 01731-1805

Ref Item 13b. Classified AIS processing is expected at the contractor facility equipment type, location, and procedures must be approved by ESC/NI60. Expiration Date of Contract: No later than TBD.

Ref Item 13c The National Industrial Security Program Operating Manual (NISPOM), January 1995 applies to this contract.

Attachment 1 SCI ADDENDUM

Ref Item 13A. This contract requires additional security requirements established for Sensitive Compartmented Information (SCI) in accordance with (IAW) DOD Directive TS-5105.21 (M-3)/DOD S-5105.21(M-1). AF MAN 14-304. AF MAN 14-304 and M-1 provides the necessary guidance for physical, personnel, and information security measures and is part of the security specifications for this contract.

Ref Item 13B. This contract will be administered under the following documents, with subsequent versions or changes.

1. AF MAN 14-304
2. DOD Directive S-5105.21 (M1)
3. DOD Directive TS-5105.21 (M3)
4. Chairman of the Joint Chiefs of Staff Emergency Action Procedures, Volume I,
5. National Military Command System (NMCS) Security Classification Guide

Ref Item 13C. Inquiries pertaining to classification guidance on SCI will be directed to the responsible ESC contract monitor, indicated in Item 14Q. Any SCI or SCI-derived material generated under this contract will be reviewed by the contract monitor for proper classification prior to final publication and distribution. The responsible Special Security Office as designated in Item 14O, will provide assistance as required.

Ref Item 14A. SCI data furnished to or generated by the contractor will require special security handling and controls beyond those in the national industrial security program-operating manual (NISPOM). These supplemental instructions will be furnished and/or made available to the contractor through the contract monitor by the User Agency Special Security Office (SSO ESC). Contract monitors and Contractor Special Security Officers (CSSOs) will comply with all requirements outlined in AF MAN 14-304 AND M1. The CSSO will complete an annual self-inspection of all SCI related contract activity using the self-inspection checklist located in the M1. The self-inspection should take place in January of each year and a report of the self-inspection and all discrepancies noted will be forwarded to SSO ESC before the end of that month.

Ref Item 14B. Contractor billets are required to perform on this contract. The contract expiration date is TBD.

Ref Item 14C. Names of contractor personnel requiring access to SCI will be submitted to the contract monitor for approval. Upon written approval by the contract monitor, forms requesting Single Scope Background Investigation (SSI) will be prepared in accordance with the NISPOM and submitted to DSS.

Ref Item 14D. The contractor will establish and maintain an access list of those employees working on this contract. A copy of this list will be furnished to the contract monitor.

Ref Item 14E. The contractor will advise the SSO, through the SCI contract monitor, immediately upon reassignment of personnel to other duties not associated with this contract.

Ref Item 14F. Release of Information: SCI shall not be released to contractor employees without specific release approval of the ESC Senior Intelligence Officer (SIO) or the originator of the material when applicable. SCI with restrictive caveats (ORCON, PROPIN, etc.) will be released to contractors only when originator approval has been obtained. This approval shall be obtained through SSO ESC based on approval and certification of "need-to-know" by the contract monitor. SCI documentation, or other material concerning this contract will not be discussed with or released to any individual, subcontractor, agency (including Federal government agencies and employees), and contractor employees not working on the contract without prior approval from the contract monitor.

Ref Item 14G. Any SCI data released to or generated by the contractor in support of the contract remains the property of the DOD Department, agency, or command that released it. The contractor will maintain a record of all SCI released to his custody under this contract and upon completion/cancellation of the contract, must return all such materials to SSO ESC. A copy of this record will be sent to the SCI contract monitor quarterly and to SSO ESC annually for their review. This applies to all data and materials, including working papers and notes. SCI inventories will be conducted IAW AFMAN 14-304 and M1.

Ref Item 14H. The contractor will not reproduce any SCI related to this contract without the written permission of the contract monitor. When such permission has been granted, the contractor will control and account for such reproductions in the same manner as pertains to originals. Reproductions of hard copy SCI documents in their entirety is not permitted.

Ref Item 14I. If the contractor utilizes an SCI Facility (SCIF), the SCIF must be built IAW Director of Central Intelligence Directive (DCID) 1-21 standards and an SCI accreditation message must be on file within the SCIF. If the SCIF is accredited through other than HQ AFMC, the contract monitor will generate a Co-Utilization Agreement (CUA). SCI material associated with this contract shall be separately stored and maintained only in such properly accredited facilities and approved safes at the contractor location. The supporting Special Security Office is US Army Contractor Support Detachment, East. POC is Mr. Henry Wallen, (703) 617-7323/7324.

Ref Item 14J. This contract does require the use of Defense Courier Service (DCS); SSO ESC will validate all DCS Form 10.

Ref Item 14K. A COMSEC account is required. The Communications Security (COMSEC) Supplement (DOD 5220.022-S-1) to the NISPOM for the handling of COMSEC material, is applicable. Access to COMSEC information is restricted to US citizens holding final US Government security clearances and is not releasable to personnel granted reciprocal clearances. COMSEC information is not releasable to contractor employees who have been granted a reciprocal clearance.

Ref Item 14L. This contract does require electronic processing of SCI. The security provisions of DCID 6/9, DIAM 50-4 and AF MAN 14-304 and M-1 apply and are part of this contract. No electronic processing will take place in the SCIF until Communications/EMSEC and Automated Information System (AIS) accreditation messages are on file within the facility.

Ref Item 14M. The CSSO must coordinate with the SCI contract monitor prior to subcontracting any portion of SCI efforts involved in this contract. A separate DD Form 254 for the subcontractor shall be processed and approved, and separate subcontractor billets shall be obtained before any work can be performed. Subcontractors cannot use the prime contractor's SCI billets.

Ref Item 14N. The contractor will not use references to SCI accesses, even by unclassified acronyms, in advertising, promotional efforts, or recruitment of employees.

Ref Item 14O. The following activity (SSO ESC) is designated as the User Special Security Office for SCI requirements in accordance with AF MAN 14-304 and M-1.

ESC/INS
102 Barksdale Street
Hanscom AFB, MA 01731-1805
Phone: DSN 478-2187/88 Commercial: (617) 377-2187/2188

Ref Item 14P. The User Agency Special Security Officer (SSO) is

DARLENE A. CEROVAC
Asst Chief, Special Security Office
Directorate of Intelligence
Electronic Systems Center (AFMC)

Date: _____

Ref Item 14Q. The Contract Monitor for SCI/SAR is:

Mr. Mark D. Hutton
ESC/NDAS
11 Eglin Street
Hanscom AFB, MA 01731-2120
Phone: DSN 478-2683 Commercial (781) 377-2683

Ref Item 15A. The Assistant Chief of Staff for Intelligence, Surveillance and Reconnaissance, Headquarters United States Air Force (HQ USAF/XOI) has exclusive responsibility for all SCI classified material released or developed under this contract and held within the contractor's SCIF. DIA is responsible for security inspection of all SCI and non-SCI classified material released to or developed under this contract and held within the contractor's SCIF

Ref Item 15B. Although DIA is primarily responsible for inspection of all classified material associated within a contractor's SCIF, the SAO will also inspect such material. The only material that the SSO will not inspect is SAR material the SSO USAF/INSC has approved for storage within the contractor's SCIF.

**Addendum for
FOR OFFICIAL USE ONLY (FOUO)**

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 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.**

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 and 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 by First-class mail or parcel post. Bulky shipments may be sent by fourth-class mail.

6. DISPOSITION AND 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.

Attachment 3

Reference Item 11i. EMISSION Security (EMSEC) Requirements

1. The contractor shall ensure that compromising emanations conditions related to this contract are minimized. The following procedures relate to classified processing conducted within the US. Within NATO countries, prime contractors and sub-contractors using contractor or NATO-controlled equipment will adhere to NATO requirements for Emission Security (EMSEC) procedures. Contractors operating US-only equipment, whether in a NATO-controlled facility or US-controlled facility, must comply with Air Force EMSEC procedures as specified by the cognizant EMSEC Manager.
2. For contracts which require the processing of classified information in a contractor facility, the contractor shall provide countermeasure assessment data to the Contracting Officer (CO), in the form of an EMSEC countermeasures assessment Request (ESAR). The ESAR shall provide only specific responses to the data required in paragraphs 4.1 - 4.4, below. The contractor's standard security plan is unacceptable as a "stand-alone" ESAR response. The ESAR information will be used to complete an EMSEC assessment and countermeasures review of the contractor's facility, to be performed by the government EMSEC authority using current Air Force EMSEC directives.
3. The contractor will not process classified information until an ESAR is contractually submitted, the EMSEC assessment and countermeasures review have been conducted, and the system has been accredited/approved by the Cognizant Security Agency (CSA) in accordance with Chapter 8 of the NISPOM.
 - 3.1 Recognizing that contractors utilize Information Systems (IS) for multiple contracts, ESAR assessments compiled and approved for a particular system under one ESC contract are considered approved under other existing, follow-on and new ESC contracts for that particular contractor, as long as no changes are made to the security profile of the IS. The approval(s) should be kept on file for all affected contracts.
 - 3.2 Any requests for interim approval to process classified information, until ESAR information can be submitted and EMSEC procedures completed must be approved by the CSA. Such interim approval should not exceed 90 days.
4. When any of the information required in paragraphs 4.1 – 4.4 below changes (such as equipment, location or classification level), the contractor shall notify the contracting officer of the changes so an EMSEC Reassessment may be accomplished. The contractor shall submit to the System Program Office (SPO) or contracting officer a new ESAR, specifically identifying the configuration changes. It should be submitted at least thirty (30) days before the changes are projected to occur. The provisions of Paragraph 3 apply to these changes.

4.1. SYSTEM DESCRIPTION

- 4.1.1 SYSTEM/FACILITY: Full name and address of company submitting request and RFP/contract number and duration. Also provide a brief title identifying the overall system or facility (e-g. XYZ Missile word-processing system, ABC aircraft interactive graphics system, etc.).
- 4.1.2 LOCATION: Provide the following information for the facility where processing will take place.
 - 4.1.2.1. Identify the address (including city, state, zip code, facility, building and room number) where the system or facility is located. If the address is the same as 4.1.1., only indicate the building and room number where the equipment is located.
 - 4.1.2.2. Make, title, and attach drawings/maps showing the inspectable space (See 4.1.2.2.1), Controlled Access Areas (See 4.1.2.2.2), and floor layout of the RED and BLACK equipment. The floor layout of the equipment (RED and BLACK) should include the locations of any transmitters, transceivers, and cryptographic equipment, as well as RED and BLACK IS. The drawing may be free hand. Include the scale (roughly). Indicate on the map surrounding buildings to a distance of 200 meters. Identify significant occupants, organizations, and activities in the buildings within 200 meters. If the U.S. Government or the contractor identified in 4.1.1 above does not wholly occupy the building containing the RED equipment, identify and indicate the location of those other occupants.
 - 4.1.2.2.1. **Definition of Inspectable Space**—The three-dimensional space surrounding equipment that processes classified or sensitive information within which TEMPEST exploitation is not considered practical, or where legal authority to identify or remove a potential TEMPEST exploitation exists.
 - 4.1.2.2.2. **Definition of Controlled Access Area (CAA)**—The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access

and are either escorted by authorized persons or are under continuous physical or electronic surveillance.

4.2. RESPONSIBLE PERSONNEL:

4.2.1 INFORMATION SYSTEM SECURITY MANAGER (ISSM): Provide name, title, office symbol and telephone number. Include the same for the Company Appointed EMSEC (TEMPEST) Authority, if applicable.

4.2.2 SYSTEM CUSTODIAN: If different from above, provide name, title, and office symbol and telephone number.

4.3. OPERATIONAL RISK:

4.3.1 Identify the highest level of classified processing.

4.3.2 Provide an estimate of the total classified processing volume in a given measure of time. The estimate can be in hours per day, pages of classified generated per week, or megabytes or gigabytes processed per day/month. (e.g., 2 hrs/day, 15 pages/mo, or 320 mb/week) , AND a percentage of total material processed for each level (e.g. 10% Top Secret; 55% Secret; 20% Confidential; 15% unclassified).

4.4 EQUIPMENT:

4.4.1 List the manufacturer and exact model number, nomenclature (terminal, disk drive, video system, etc.) and quantity of each equipment involved in classified processing. Do not provide a complete inventory of all the company's processing equipment.

4.4.2 List any encryption equipment (i.e., STU-III, KG-84, KG-194, etc.), that might be used for processing and transmission of classified information.

4.4.3. List any transmitters/transceivers (SATCOM, RF, UHF/VHF, WLAN, etc.) operating in the area (same room and adjacent rooms) of the equipment processing classified information, and indicate their approximate distance from the RED equipment.

5.0 EMSEC is applied on a case-by-case basis and further information may be required to complete the ESAR; should this be the case, the contractor shall provide this information to the contracting officer, PMO or SPO when requested.

6.0 Current requirements of AFI 33-214 Vol. 2 and AFI 33-203 dictate that the information used to complete the EMSEC Assessment and Countermeasures Review be validated annually. The ISSM shall certify annually to the PMO, SPO, or contracting officer that no changes to the information provided in paragraphs 4.1 through 4.4 of the ESAR have occurred.

7.0 The prime contractor shall ensure that this EMSEC requirement is provided to all subcontractors and/or vendors. The subcontractors and/or vendors shall comply with these EMSEC requirements when classified processing related to this contract is necessary. Subcontractors and/or vendors will provide their ESAR through the prime contractor to the government contracting officer.

8.0 WITH THE EXCEPTION OF 3.2 ABOVE, CLASSIFIED PROCESSING WILL NOT BE DONE UNTIL THE ABOVE PROCEDURES ARE COMPLIED WITH AND THE IS HAS BEEN ACREDITED BY THE COGNIZANT SECURITY AGENCY (CSA).

9.0 If you have any questions feel free to contact Mr. Alfred Knoll, Hanscom AFB EMSEC Manager.

Mailing Address: ESC/NI6O
50 Hamilton Street
Hanscom AFB, MA
01731-1621

E-Mail: Alfred.Knoll@hanscom.af.mil
SIPRNet: Alfred.knoll@hanscom.af.smil.mil
Phone: (781) 377-4716
Fax Number: (781) 377-0562
STU-III Number: (781) 377-3497

Attachment 4

ADDENDUM FOR GENERAL INTELLIGENCE MATERIAL/FOREIGN DISCLOSURE

1. Special Requirements for General and Foreign Intelligence Material. In addition to the requirements and controls for classified material, the Director, Central Intelligence, sets up additional requirements and controls for intelligence in the possession of contractors. The contractor must:

- a. Maintain control of all intelligence materials released in his or her custody in accordance with DOD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM), January 1995, paragraphs 5-200, 201 and 202 for control. Contractor agrees that all intelligence material released, all reproductions and other material generated (including reproductions) are the property of the US Government.
- b. Maintain control of all reproduced intelligence data in the same manner as the original.
- c. Destroy intelligence materials in accordance with approved methods identified in the NISPOM.
- d. Restrict access to those individuals with a valid need-to-know who are actually providing services under the contract. Further dissemination to other contractors, subcontractors, or other government agencies and private individuals or organization is prohibited unless authorized in writing by the Contracting Officer's Representative (COR) with prior approval of the Unit IN/SIO.
- e. Not release intelligence data to foreign nationals or immigrant aliens, regardless of their security clearance or contract status, without advance written permission from the COR, Foreign Disclosure Policy Office and Unit IN/SIO.
- f. Ensure that each employee having access to intelligence material is fully aware of the special security requirements for this material.

2. Returning Intelligence to the Air Force. Contractors must return intelligence data to the COR at the termination or completion of a contract unless the COR has provided written approval for the contractor to retain for an additional two years. If retention is required beyond the two year period, the contractor must again request and receive written retention authority from the COR. If the COR grants retention authority, the COR must provide a copy of the written approval to the Unit IN/SIO.

3. Release of Classified and Unclassified Intelligence Information to Foreign Government and Their Representatives. Any military activity or defense contractor receiving a request from a foreign government or a representative thereof, for intelligence data about this program, shall forward the request to the Unit IN/SIO for coordination with the cognizant foreign disclosure office. Information released under Foreign Military Sales (FMS) must comply with the specific USAF disclosure guidance issued for the specific FMS customer.