

**DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION**

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED

TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

TOP SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

<input type="checkbox"/>	a. PRIME CONTRACT NUMBER	
<input type="checkbox"/>	b. SUBCONTRACT NUMBER	
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER 04-05-MLK	DUE DATE (YYYYMMDD) 20040412

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

<input checked="" type="checkbox"/>	a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD) 20040224
<input type="checkbox"/>	b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)
<input type="checkbox"/>	c. FINAL <i>(Complete Item 5 in all cases)</i>	DATE (YYYYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? YES 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? YES 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 *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE TBD	b. CAGE CODE TBD	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> TBD
---------------------------------------	---------------------	--

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE N/A	b. CAGE CODE N/A	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> N/A
---------------------------------------	---------------------	--

8. ACTUAL PERFORMANCE

a. LOCATION N/A	b. CAGE CODE N/A	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> N/A
--------------------	---------------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

The purpose of this research and development effort is to demonstrate hardening technologies in Intelligence Surveillance and Reconnaissance (ISR) and targeting system configurations. The effort will concentrate on technologies that provide protection capability in the visible, near infrared, short wave infrared, mid wave infrared, and long wave infrared regions. Both jamming and damage protection technologies will be demonstrated.

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		<input checked="" 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 checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT		<input checked="" type="checkbox"/>
g. NATO INFORMATION		<input checked="" type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS		<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input checked="" type="checkbox"/>		j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	
i. LIMITED DISSEMINATION INFORMATION		<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		<input checked="" type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>		l. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/>
k. OTHER <i>(Specify)</i>		<input checked="" type="checkbox"/>			

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)

ASC/PAX Bldg 14, 1865 4th Street, WPAFB, OH 45433-7129
(937) 255-2776 FAX (937) 656-4022 <http://ascpa.public.wpafb.af.mil >

Public release of Sensitive Compartmented Information (SCI) 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.)

The National Industrial Security Program Operating Manual (NISPOM), Jan 95, applies to this solicitation.

- a. Ref Blk 10e(1): Contractor requires access to SCI materials; SCI security requirements apply, see SCI addendum for details.
- b. Ref Blk 10e(2): Contractor will require access to intelligence information and must comply with AFI 14-303/AFMC Supplement 1. The Program Manager has determined that disclosure does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. The contractor will submit the AFMC Form 210 to AFRL/SNOY for approval prior to granting access.
- c. Ref Blk 10j: For Official Use Only (FOUO) applies. See addendum.
- d. Ref Blk 11c: Any classified information generated in the performance of this contract shall require the contractor to apply derivative classification and markings consistent with the source material or be governed by the current version of the Projects 2100/4348 Laser Hardened Materials Security Classification Guide, dated 30 Sept 1997, Letter Change 1, dated 30 Sep 99, Letter Change 2, dated 3 Jan 00, OPR: AFRL/MLPJ Special Considerations Apply. See Addendum. SCG will be provided under separate cover.
- e. Ref Blk 11d: This contractor is required to provide adequate and approved storage for classified hardware or material to the level of TOP SECRET which because of size or quantity cannot be safeguarded in an approved storage container.
- f. Program Manager - Rafael Reed, AFRL/MLPJ (937) 255-3808 ext 3160.
- g. Ref Blk 17f (DISTRIBUTION): 88 SFS/SFAS

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.)

- a. Ref Blk 10e(1): SCI security requirements apply, see SCI addendum for details. COR is _____, ___ billets.
- b. Ref Blk 11j: OPSEC requirements apply. CIs will be provided to contractor under separate cover and updated as required.

15. **INSPECTIONS.** Elements of this contract are outside the inspection responsibility of the cognizant security office. Yes No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. **CERTIFICATION AND SIGNATURE.** Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below. *dh*

a. TYPED NAME OF CERTIFYING OFFICIAL		b. TITLE		c. TELEPHONE (Include Area Code)	
William Beeman		Contracting Officer		(937)656-9003	
d. ADDRESS (Include Zip Code)		88SFS/SFAS COORDINATION RFP-ONLY			
AFRL/MLKM 2310 8th St Bldg 167 WPAFB OH 45433-7801					
e. SIGNATURE		7. REQUIRED DISTRIBUTION			
<i>William O. Beeman</i> <i>Sharon Bemis 24 Feb 01</i>		<input checked="" type="checkbox"/> a. CONTRACTOR			
		<input type="checkbox"/> b. SUBCONTRACTOR			
		<input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR			
		<input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION			
		<input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER			
		<input checked="" type="checkbox"/> f. OTHERS AS NECESSARY			

ADDENDUM TO DD FORM 254 (Block 10e(1))
SENSITIVE COMPARTMENTED INFORMATION (SCI) CLAUSES

1. **Reference Block 14:** AFMAN 14-304; DoD 5105.21-M-1; DCID 6/3, 6/4, 6/8, 6/9, and 1/19; JDCSISSS; and DIAM 50-4 provide the necessary guidance for physical, personnel, industrial, information, and information systems security measures and is part of the Sensitive Compartmented Information (SCI) security specifications for the contract.

2. SCI will not be released to contractor employees without the specific release approval by the originator of the material as outlined in the governing directives and based on prior approval and certification of "need-to-know" by the Contracting Officer's Representative (COR):

_____ (Name)

_____ (Office Symbol)

_____ (Phone)

3. Names of contractor personnel requiring access to SCI and justification for SCI billets will be submitted for coordination and action to SSO ASC/INS after the contract monitor approval/concurrence. Upon receipt of written approval from the COR, the Contractor Special Security Officer (CSSO) may submit the necessary forms to Defense Security Service (DSS) for a Single Scope Background Investigation (SSBI) for those personnel nominated for SCI access in accordance with the National Industrial Security Program Operating Manual (NISPOM).

4. This contract requires a total of ____ SCI contract billets in order to fulfill contractual obligations incurred. SCI access is subject to US Government review and approval as outlined in the aforementioned SCI security regulations. Upon completion or cancellation of the contract, the CSSO will debrief all personnel not required for contract closeout and those billets will be disestablished.

5. The CSSO must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract. Further dissemination to other contractors, sub-contractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the releasing agency.

6. SCI materials furnished in support of this contract remains the property of the DoD department or command that released it. Upon completion or cancellation of the contract, all SCI materials furnished will be returned to the direct custody of the originator of the materials.

7. Classified foreign intelligence materials must not be released to foreign nationals or immigrant aliens whether or not they are also consultants, US contractors, or employees of the contractor, regardless of the level of their security clearance, except with advanced written permission from the originator.

8. Inquiries pertaining to classification guidance on SCI will be directed to the COR listed in para 2 above. SCI security management issues shall be directed to SSO ASC/INS, phone (937) 255-3932, DSN prefix 785.

9. An SCI Facility (SCIF) meeting the physical security requirements outlined in DCID 6/9 must be either used for contract work or established and maintained at the contractor location. All SCI used for this contract shall be stored, handled, and maintained in a SCIF, be it the local contractor SCIF or similarly SCI-accredited facilities used by the contractor. Address of SCIF for contract execution: _____

10. For contract work within a contractor established SCIF, information systems (computers), electronic connectivity, and similar electronic methods of storing and communicating within and outside the SCIF must be in compliance with DCID 6/3, DIAM 50-4, the JDCSISSS, and any additional instructions issued by DIA/DAC-2A, HQ AFMC/INS, and SSO ASC/INS.

11. The CSSO must maintain accountability for all classified foreign intelligence materials released to their custody.

12. The CSSO must not reproduce classified foreign intelligence without advance approval of the releasing agency. If permission is granted, each copy will be controlled in the same manner as the original. The CSSO must not destroy any classified foreign intelligence without advance approval of the releasing agency.

13. **Reference Block 15:** This contract requires access to SCI. If the contractor has established a SCIF, the Defense Intelligence Agency (DIA) and its designees are responsible for all inspections of the contractor SCIF and SCI security management program for ensuring compliance with all SCI security regulations and policies.

Effective: 27 February 2003

ADDENDUM TO DD FORM 254 (Blocks 10e(1) and 11c)
SPECIAL CONSIDERATIONS
(AFMAN 33-214V EXTRACT)

NOTE: These considerations are not applicable to performance within a Sensitive Compartmented Information Facility (SCIF). See paragraph 10 of SCI addendum for guidance.

3.4. Special Items. People may innocently introduce other radio devices, such as pagers, hand-held portable transceiver radios, cellular telephones, cordless telephones, and cordless microphones into the area processing classified information with disastrous results. Also, alarm systems may use radio transmitters to alert remotely located security or fire-fighting teams.

3.4.1. Hand-Held Radios. These countermeasures are required. Hand-held radio transceivers used with intrabase radios and land mobile radios deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or separate it 2 meters from classified processors: no transmissions are allowed. If the person carrying the device is a short-term visitor, it is not necessary to turn off the radio because the visitor usually moves about in the facility. Infrequent transmissions are allowed, but only for short durations.

3.4.2. Beepers and Pagers. These countermeasures are required. Beepers and pagers deserve special consideration because of their unique operational applications. A person may carry these devices into an area where classified information is processed. If the person carrying such a device works in the facility, either turn off the device and use the telephone or keep the device 2 meters from classified processors. If the person carrying the device is a short-term visitor, it is not necessary to turn off the device because the visitor usually moves about in the facility. If the device has a transmit capability, follow the instructions for hand-held radios.

3.4.3. Alarm Systems. These countermeasures are required. The mode of operation of alarm systems radio frequency transmitters will determine their treatment. Any such transmitter with a continuous transmit mode or a high duty cycle (transmits most of the time) must meet the same separation requirements as all other fixed transmitters; follow the applicable guidance in paragraph 3.3. If they do not meet these requirements, exclude them from operating in the classified information processing area. Low duty cycle (transmits short bursts infrequently) systems are not considered hazards and require no special treatment.

3.4.4. Cellular Telephones. These countermeasures are required. When a cellular telephone is used as an operational necessity separate it 5 meters from RED equipment. When the cellular telephone is a personal asset, its use is prohibited. Disable the unit from receiving calls or separate it 10 meters from RED processors. Cellular telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

3.4.5. Cordless Telephones. These countermeasures are required. When a radio frequency cordless telephone is used as an operational necessity, separate it 5 meters from RED equipment. When the cordless telephone is a personal asset, its use is prohibited. Disable the personal cordless telephone from receiving calls or separate it 10 meters from RED processors. There are no separation requirements for infrared cordless telephones. Cordless telephones are excluded from operating within 10 meters of the classified information processing area when the facility is located outside the United States.

3.4.6. Cordless Microphones.

3.4.6.1. Radio Frequency Cordless Microphones. These countermeasures are required. When a radio frequency cordless microphone, encrypted or unencrypted, is used for briefing either classified information or unclassified information, separate it 10 meters from RED equipment. Using unencrypted radio frequency cordless microphones for classified briefings is prohibited.

3.4.6.2. Infrared Cordless Microphones. These countermeasures are required. Using an infrared cordless microphone for briefing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

3.5.7. Cordless Accessories. These countermeasures are required. When a radio frequency cordless accessory such as a keyboard or a mouse is used, separate it 5 meters from RED equipment. Radio frequency cordless accessories cannot be used to process classified information unless encrypted.

3.4.8 Wireless Local Area Networks (LAN). These countermeasures are required. When a radio frequency wireless LAN is used, separate the transmitter and receiver units 5 meters from RED equipment.

3.4.9 Infrared LANs. These countermeasures are required. An infrared LAN processing classified information requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

3.4.10 Infrared Devices. These countermeasures are required. Infrared devices not covered by any subparagraph of paragraph 3.4 requires blocking the line of sight to a possible place where an adversary could detect the infrared emanations. Do not forget that smooth or shiny surfaces cause infrared signals to be reflected. The best solution is to use a closed room, keeping the doors closed and covering the windows with drapes.

NOTE: If guidance in paragraph 3.3 on Alarm signals is needed, please contact the Program Manager/Contract Monitor to obtain.

ADDENDUM TO DD FORM 254 (Block 10j)
FOR OFFICIAL USE ONLY (FOUO)
(Reference DoD Regulation 5400.7/Air Force Supplement, 22 July 1999)

1. **GENERAL:** FOUO is information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public because disclosure would cause a foreseeable harm to an interest protected by one or more of the Freedom of Information Act (FOIA) exemptions 2 through 9. Additional information on FOUO may be obtained by contacting the User Agency. FOUO is assigned to information at the time it is created in a DoD Agency or derivatively as instructed in a Security Classification Guide.
2. **MARKING:**
 - a. FOUO information received (**released by a DoD component**) should contain the following marking, when received: ***THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER FOIA. EXEMPTION(S) _____ APPLIES/APPLY.***
 - b. Mark an unclassified document containing FOUO information "FOR OFFICIAL USE ONLY" at the bottom of each page containing FOUO information and on the bottom of the front page or front cover (if any) and on the back of the last page and on the back cover (if any). Each paragraph containing FOUO information shall be marked as such.
 - c. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate. An individual page that contains FOUO information but no classified information shall be marked "FOR OFFICIAL USE ONLY" at the top and bottom of the page, as well as each paragraph that contains FOUO information. NOTE: For "production efficiency" the entire document may be marked top and bottom with the highest level of classification contained within it, as long as every paragraph is marked to reflect the specific classification of the information it contains.
 - d. Mark other records, such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.
 - e. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.
3. **DISSEMINATION:** FOUO may be disseminated between officials of DoD Components, DoD contractors, consultants and grantees to conduct official business for DoD. Recipients shall be made aware of the status of such information **and transmission shall be by means that preclude unauthorized public disclosure.**
4. **TRANSMISSION:** FOUO information shall be transmitted in a manner that prevents disclosure of the contents. When not commingled with classified information, it may be sent via first-class mail or parcel post. Bulky shipments, i.e. testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail. FOUO information may also be sent over facsimile equipment; however, when deciding whether to use this means, balance the sensitivity of the records against the risk of disclosure. Consider the location of sending and receiving machines and ensure authorized personnel are available to receive the FOUO information as soon as it is transmitted. Transmittal documents shall call attention to the presence of FOUO attachments. FOUO information may also be sent via e-mail, if it is sent via a system that will prevent unintentional or unauthorized disclosure.
5. **STORAGE:** To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when normal internal building security is provided. When there is no internal building security, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked containers such as file cabinets, desks, or bookcases. *Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.*
6. **DESTRUCTION:** When no longer needed, FOUO information shall be disposed of by any method that will preclude its disclosure to unauthorized individuals.