

APPENDIX E

CONTROL OF COMPROMISING EMANATIONS (TEMPEST)

Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

(Updated 23 October 2003)

1. Reference:

- a. DOD 5220.22-M, National Industrial Security Program Operating Manual, January 1995.
- b. Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U).

2. In accordance with guidance referenced above, a TEMPEST Countermeasure Review (TCR) will only be employed where a threat of exploitation exists. A TCR must be performed by a Certified Tempest Technical Authority (CTTA) 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 completed DA Form 7453 Facility Technical Threat Assessment (FTTA) Worksheet will be completed IAW with Confidential Regulation AR 381-14, Technical Counterintelligence (TCI), 30 September 2002 (U) only if either of the following conditions applies:

- 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.

APPENDIX F

SAFEGUARDING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION
Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

1. The "FOR OFFICIAL USE ONLY" 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 may be 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 instructions 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 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 possible.
5. DISSEMINATION: Contractors may disseminate "FOR OFFICIAL USE ONLY" information to their employees and subcontractors who have a need for the information in connection with a classified contract.
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 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.
7. TRANSMISSION: "FOR OFFICIAL USE ONLY" information may be sent via first-class mail or parcel post. Bulky shipments may be sent fourth-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 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.
10. Point of contact is the DCSINT, DSN 987-5875, Commercial (732) 532-5875.

APPENDIX G

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

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, computations 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, or his/her duly appointed representative.

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. 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.
4. The following downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2

DECLASSIFY ON: Source Marked "OADR" (if generated before 1 April 1995)

DATE OF SOURCE: (Date of document from which information is derived)

5. 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 granted 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.
6. 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 without the express written permission of the Director, NSA, is strictly prohibited.
7. Recipients of COMSEC information under this contract may not release information to subcontractors without permission of the User Agency.
8. The requirements of DOD 5220-22-S are applicable to this effort.
9. Additional notices 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 NATIONALS 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."
10. Point of contact is the DCSINT, AMSEL-MI.

CONTRACT #
SOLICITATION # **W15P7T-04-R-L216**

APPENDIX—H

INTELLIGENCE MATERIALS ACCESS REQUIREMENTS

Provided by the Deputy Chief of Staff for Intelligence (DCSINT)

(Updated 2 June 2004)

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the Deputy Chief of Staff for Intelligence (DCSINT), U.S. Army Communications-Electronics Command (USA CECOM). Any intelligence materials so provided will be disseminated solely by the DCSINT, 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 CECOM, DCSINT.
2. All requests for access to intelligence materials will adhere to the following guidelines:
 - a. Prime contractor requests for intelligence materials access will be sent to the Program/Project Manager (PM) of the User Activity on official business letterhead with an enclosed copy of the approved DD Form 254.
 - b. Subcontractor requests for access to intelligence materials will be forwarded by the prime contractor to the PM on official business letterhead with an enclosed, approved DD Form 254 for the relevant subcontract.
 - c. PM of the User Activity will forward request through the Contracting Officer (KO) on official letterhead with the appropriate DD Form 254 and all substantiating documents attached, to be forwarded to DCSINT for review and concurrence.
3. Point of contact is CECOM DCSINT, AMSEL-MI.

APPENDIX I

US ARMY SCI ADDENDUM TO DD FORM 254, 18 February 2004

XXX (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, US Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff (DCS), G-2 as the Cognizant Security Authority (CSA) for the US Army, has exclusive security responsibility for all SCI released to the contractor or developed under the contract and held within the Contractor's SCI Facility (SCIF) or Co-utilization Agreement (CUA) SCIF. The Defense Intelligence Agency (DIA) has security inspection responsibility for SCI and the Defense Security Service (DSS) retains responsibility for all collateral information released or developed under the contract and held within the DoD Contractor's SCIF. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SCI, and are part of the security classification specification for this contract:

XXX DOD 5105.21-M-1, SCI Security Manual, Administrative Security

XXX Signals Intelligence Security Regulations (SISR) (Available from the CM)

_____ Imagery Policy Series (Available from the CM)

_____ DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems

_____ DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities

_____ DIAM 50-4, DOD Intelligence Information System

_____ DIAM 50-24, Security for Using Communications Equipment in a SCIF.

_____ AR 25-2, Information Assurance

XXX AR 380-28, DA Special Security System

_____ AR 380-381, Special Access Programs (SAPS)

XXX Army Handbook for SCI Contracts

_____ Other

XXX (2) Contract estimated completion date: _____ (NOTE: Section "F" of the contract normally provides the Period of Performance. Option years are not to be included, as an option is not valid until exercised by the government.)

XXX (3) The name, telephone number, email address and mailing address of the Contract Monitor (CM) for the SCI portion of this contract is: _____ (Additionally, identify the Security POC & phone number and email address at the contractor's/subcontractor's location):

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the CM for approval and then to HQ INSCOM, ACofS Security, G2, and Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

XXX (5) The contractor will submit the request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the Contractor Support Element at least ten (10) working days prior to the visit.

XXX (6) The contractor will not reproduce any SCI related material without prior written permission of the CM.

_____ (7) Security Classification Guides or extracts are attached or will be provided under separate cover.

_____ (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3, DIAM 50-4, and AR 25-2 (Note: Check only if item 111 indicates that a requirement exists for SCI AIS processing.)

_____ (9) This contract requires a contractor SCIF.

XXX (10) This contract requires __ (SI) __ (TK) __ (G) __ (HCS) (Add others as required)

XXX (11) The contractor will perform SCI work under this contract at the following locations:

APPENDIX J

SCI
CONTRACT MONITOR (CM)/ALTERNATE CONTRACT MONITOR (ACM)
INFORMATION

Under the provisions of DIAM 50-5, a Contract Monitor must be designated as soon as possible for all SCI Contracts. Appointment orders will be prepared by the Senior Intelligence Officer (SIO) for CECOM/Ft Monmouth. Request the following information be submitted to the Deputy Chief of Staff for Intelligence (DCSINT), ATTN: AMSEL-MI. All appointment orders will then be forwarded to the appropriate activities/personnel.

CONTRACT MONITOR

ALTERNATE

NAME:

SSN:

ADDRESS (ACTIVITY, OFFICE SYMBOL, BUILDING NO.)

(CM)

(ACM)

TELEPHONE #

DSN (CM):

(ACM):

COMM (CM):

(ACM):

CONTRACT COMPANY INFORMATION

CONTRACT NUMBER:

EXPIRATION DATE:

CONTRACT COMPANY NAME AND ADDRESS:

TELEPHONE NUMBER:

CAGE CODE:

APPENDIX K

SCI CONTRACT REQUIREMENT CHECKLIST

Appropriate personnel from the user activity, i.e., Project Leader, CM/ACM, Technical Personnel, Contracting Officers, etc., must participate in completing this checklist for all SCI contracts. Some information can be obtained from the CECOM Industrial Security Specialist, DCSINT.

Question	Yes or No Response	Date Completed
1. Obtain a draft statement of work (SOW) and SOW Number		
2. Does the SOW reflect the SCI requirement?		
3. Does the SOW identify the level of classification for Contract? If 'YES', what is the classification level?		
4. Does the SOW identify the need for contractor access to SCI? a. If yes, provide the SCI contract monitor's (CM) name, phone # b. Has the CM/ACM received appropriate training in the duties of administering an SCI contract? (date)		
5. Verify documentation prepared by the SCI CM that supports the need for contractor access to SCI a. Does the documentation fully justify the types of sensitive compartmented information needed, why the contract can't be completed without the access, and how the information will be used? b. Does the draft SOW work reflect the SCI requirements? c. Does the documentation provide estimates of the number of contractor personnel requiring access to SCI? d. What is the projected number of contractor personnel requiring SCI access? e. Has supporting documentation and name of SCI CM been provided to the SIO or appropriate security office for review of SCI requirements and preparation of SCI CM appointments?		
6. Has the approved checklist, supporting documentation and SOW been provided to the Contracting Officer or his/her security representative for preparation of and inclusion in the initial/base DD Form 254?		
7. Has the contract documentation been submitted to the INSCOM Contractor Support Element (CSE), Fort Meade, MD, for review and concurrence?		

SIO/Intelligence Office Approval _____
 Date Approved _____