

**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: <i>(x and complete as applicable)</i>		3. THIS SPECIFICATION IS: <i>(x and complete as applicable)</i>	
<input type="checkbox"/> a. PRIME CONTRACT NUMBER		<input checked="" type="checkbox"/> a. ORIGINAL (Complete date in all cases)	DATE (YYYYMMDD) 20040226
<input type="checkbox"/> b. SUBCONTRACT NUMBER		<input type="checkbox"/> b. REVISED (Supersedes all previous specs)	Revision No. DATE (YYYYMMDD)
<input checked="" type="checkbox"/> c. SOLICITATION OR OTHER NUMBER W15P7T04RA202	DUE DATE (YYYYMMDD) 20040227	<input type="checkbox"/> c. FINAL (Complete Item 5 in all cases)	DATE (YYYYMMDD)

4. THIS IS 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 The Mitre Corporation 7515 Colshire Drive McLean, VA 22102-3481	b. CAGE CODE 7L030	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> Defense Security Service 7010 Little River Turnpike, Suite 430 Annadale, VA 22003 703-428-0018
---	-----------------------	--

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 The Mitre Corporation 7515 Colshire Drive McLean, VA 22101	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>
---	--------------	---

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT
General unclassified statement of work effort: The JASON program is a group of high level technical and analytical experts, mostly university professors, that solve complex national security issues. JASON's primary work consists of providing discrete inventions to help advance specific programs and providing scientific input to existing and new research programs.

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"/>	<input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
b. RESTRICTED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input checked="" type="checkbox"/>	<input type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>	<input 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"/>	<input type="checkbox"/>
(2) Non-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
g. NATO INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input type="checkbox"/>	<input checked="" type="checkbox"/>
i. LIMITED DISSEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	l. OTHER <i>(Specify)</i>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
k. OTHER <i>(Specify)</i>	<input checked="" type="checkbox"/>	<input 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):

Public release of 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.)

All applicable provisions of DoD 5220.22M and it's supplements apply:

10.a. COMSEC material/information may not be released to DoD contractors without AT&L Program Managers approval. Contractor forward requests for COMSEC material/information to the COMSEC officer through the program office. The contractor is governed by DoD 5220.22-S COMSEC Supplement to the NISPOM in the control and protection of COMSEC material/information. Access to COMSEC material/information is restricted to U.S. citizens holding a final U.S. Government clearance. Such information will not be released to personnel holding reciprocal clearance. Appendix G

10.b. Access to RESTRICTED DATA, information which is classified and controlled under the Atomic Energy Act of 1954, or CONFIDENTIAL NUCLEAR WEAPON DESIGN INFORMATION (CNWDI) is required. A final U.S. Government Top Secret clearance is required for contract project. Contract personnel under this contract must be briefed by an appropriate government agent and follow the guidelines of DoD directive 5210.2.

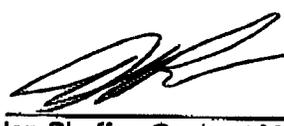
10.c. Contract personnel are permitted access to CNWDI in the performance of this contract. The government program manager designated representative will brief all contractors prior to granting access to CNWDI information. Contractor must be briefed by appropriate government agent and follow the guidelines as outline in DoD Directive 5210.2. Restricted Data shall be handled in accordance with the applicable guidance for Nuclear Weapons (Top Secret/ RD).

10.d. Access to FORMERLY RESTRICTED DATA requires a final U.S. Government clearance at the appropriate level. Program manager designated representatives will brief and grant access as required for this project.

10.e.(1). See attached SCI Release of Intelligence Information for additional security requirements. Prior approval of contractor is required for subcontracting. Access to Intelligence information requires SCI indoctrination and a final Top Secret U. S. Government clearance. Contractor will require access to DCID 6/6 and 611

The names of contractor personnel requiring access to SCI shall be submitted to the contracting officer's representative (COR) for approval. The COR will approve and coordinate visits by contractor personnel to insure satisfactory justification.

Continuation.

Approve/Disapprove: 
Alan Shaffer, Contract Monitor
Date: 2/26/2004

Concur/Nonconcur _____
Don Venneman
CSE

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 any 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

See attached SCI/Non SCI releases of Intelligence Information for additional security requirements. Access to intelligence information requires special briefings and U.S. Government Clearance at appropriate level TS/SCI. Prior approval of contracting activity is required for subcontracting. Refer to continuation page for additional security requirements.

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

The CIA/DIA has security responsibility for all SCI classified material release to or developed under this contract. DSS is relieved of security inspection responsibility for all such material. CIA/DIA is responsible for reviewing all contract's in SCIF documentation to ensure compliance with SCIF directives and regulations. DSS retains oversight/inspection responsibilities for collateral information and facility clearance requirements. Refer to continuation page for additional security requirements.

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 Grace A. Battle	b. TITLE Contracting Officer	c. TELEPHONE (Include Area Code) 732-532-1119
---	---------------------------------	--

d. ADDRESS (Include Zip Code)
Commander U.S. Army CECOM, ACQ Center
AMSEL-ACCA-RT-Y(BAT)
Fort Monmouth, New Jersey 07703

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

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-A202

APPENDIX—H

INTELLIGENCE MATERIALS ACCESS REQUIREMENTS

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

1. No Intelligence materials are to be provided in support of the contract without the prior approval of the Intelligence Support Team (IST) (Foreign Intelligence Office), 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 IST, 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 Intelligence Support Team, DCSINT, USA CECOM.
2. Point of contact is CECOM DCSINT, AMSEL-MI.

CONTRACT # _____
SOLICITATION # W15P7T-04-R-A202

APPENDIX I

US ARMY SCI ADDENDUM TO DD FORM 254, 12 February 2003

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 DoD TS-5105.21-M-2, SCI Manual, COMINT Policy

DoD TS-5105.21-M-3, TK policy

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, ACoS Security, G2, 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 380-19 (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:

CONTRACT #
SOLICITATION # W15P7T-04-02-A202

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: Alan Shaffer Barbara Brygidiae

SSN: 008-42-6506 163-42-4791

ADDRESS (ACTIVITY, OFFICE SYMBOL, BUILDING NO.)

(CM) 3040 Defense, Pentagon, Room 3D1089, Washington D.C
20301

(ACM) Same as above

TELEPHONE #

DSN (CM): 224-9604
(ACM) 224-9443

COMM (CM): 703-695-9604
(ACM) 703-614-9443

CONTRACT COMPANY INFORMATION

CONTRACT NUMBER:

EXPIRATION DATE:

CONTRACT COMPANY NAME AND ADDRESS:

Mitre Corporation
7515 Colshire Drive, McLean, VA 22102-3481

TELEPHONE NUMBER: 703-883-6316

CAGE CODE: 7L030

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	yes	Jan 21, 2004
2. Does the SOW reflect the SCI requirement?	yes	"
3. Does the SOW identify the level of classification for Contract? If 'YES', what is the classification level?	yes	"
4. Does the SOW identify the need for contractor access to SCI? a. If yes, provide the SCI contract monitor's (CM) name, phone # Alan Shaffer 703-695-9604 b. Has the CM/ACM received appropriate training in the duties of administering an SCI contract? (date) 1986	yes yes	"
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?	yes yes yes 50* yes	
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?	yes	
7. Has the contract documentation been submitted to the INSCOM Contractor Support Element (CSE), Fort Meade, MD, for review and concurrence?	TBD	

* SCI clearance through CIA

SIO/Intelligence Office Approval _____

Date Approved _____

Solicitation #W15P7T04RA202

Item 13 Continuation

10e(1). See Appendices H, I, J, K

10e (2). See attached Non SCI Release of Intelligence Information for additional security requirements. Contractor will require access to DCID 6/6.

10f. The SAP program manager OSD FFRDC Program Office (hereafter called the Contract Monitor) will provide security classification guidance for the performance of the contract. Contractor personnel must adhere to the special access requirements/procedures developed by the OPR. SAP program must approve all requests for access, and contractor must coordinate with SAP program prior to such access. (“Carve Out”)

10g. Special briefings are required for access to NATO information. Prior approval of the program manager is required for subcontracting. Access to NATO information requires a FINAL U.S Government clearance at the appropriate level and special briefings. “Access to COSMIC Top Secret information is required.”

10h. Prior approval of the OSD FFRDC Program Office is required for access to foreign government information for this project. Prior approval of the COTR is required for subcontracting.

10j. FOR OFFICIAL USE ONLY INFORMATION (FOUO): FOUO Information provided under this contract shall be safeguarded as specified in DoD 5400.7-R 1 Protecting For Official Use Only (FOUO) Information.” Appendix F

10k. All contractor personnel under this contract who have access to classified information must possess a final U.S. Top Secret clearance. The director of the OSD FFRDC Program Office (hereafter called the Contract Monitor) will provide security classification guidance for the performance of this contract.

11c/d. Contract is for technical research, development, and test support. Actual knowledge of generation or production of classified information is required for performance of this contract. Cleared personnel are required to perform this service because access to classified information cannot be precluded, All material generated by the contractor (e.g., correspondence, drawings, models mock-up, photographs, schematics, status/progress reports, engineering notes/computations, computer software training aids, etc.) shall be classified according to its own content. The contractor is not authorized to release classified information to any activity or person, including sub-contractors, without the government Contracting Officer’s written approval. Only with the expressed permission of the governments Contracting Officer may the contractor reproduce any classified information/material. All requirements for control and

Solicitation #W15P7T04RA202

accounting for original documentation and copies apply.

11f. Contractor will require access to classified information outside the U.S. to include its possessions and Trusted Territories. The government program manager will provide travel orders and direction prior to departure. Most work occurring in Washington, DC and San Diego, California.

11g. Contractor is authorized use of DTIC services. Contractor must prepare and process a DD Form 1540 and DD Form 1541 for such access. Contracting officials, with concurrence of the program manager/project manager, must review and approve contractors need to know prior to approving the DD Form 1540 and DD Form 1541. Certification of need-to-know and use of DTIC field of interest register for the acquisition of reference materials classified through Top Secret/RD, disclosures authorizations, and visits clearance approvals, fall under the responsibility of the Contract Monitor (CM).

11h. Contractor must forward request for COMSEC material/information through government program manager to COMSEC monitor. Contractor is responsible for accountable of COMSEC information and must provide a complete inventory as required by COMSEC account manager. Secure communications (e.g., KG. STU-III and/or other similar encryption technologies are authorized for this contract.) Appendix 6.

11j. OPSEC requirements are applicable to the contractor's SAP procedures but only if specified by the SAP Program Office.

11k. Contractor must obtain written approval from the contracting activity and provide the request for DCS services to Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD. 20755-5370. Prior approval of the contracting activity is required before granting subcontractor use of DCS services.

Program Manager _____

Servicing Security Activity/SSO _____

NATO Program Manager _____

Restricted Data Program Manager _____

SAP Program Manager _____

Contract expiration date _____

Solicitation #W15P7T04RA202

accounting for original documentation and copies apply.

11f. Contractor will require access to classified information outside the U.S. to include its possessions and Trusted Territories. The government program manager will provide travel orders and direction prior to departure. Most work occurring in Washington, DC and San Diego, California.

11g. Contractor is authorized use of DTIC services. Contractor must prepare and process a DD Form 1540 for such access. Contracting officials, with concurrence of the program manager/project manager, must review and approve contractors need to know prior to approving the DD Form 1540. Certification of need-to-know and use of DTIC field of interest register for the acquisition of reference materials classified through Top Secret/RD, disclosures authorizations, and visits clearance approvals, fall under the responsibility of the Contract Monitor (CM). *ADD FORM DD FORM 1541*

11h. Contractor must forward request for COMSEC material/information through government program manager to COMSEC monitor. Contractor is responsible for accountable of COMSEC information and must provide a complete inventory as required by COMSEC account manager. Secure communications (e.g., KG. STU-III and/or other similar encryption technologies are authorized for this contract.) *Appendix 6.*

11k. Contractor must obtain written approval from the contracting activity and provide the request for DCS services to Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD, 20755-5370. Prior approval of the contracting activity is required before granting subcontractor use of DCS services.

Program Manager *[Signature]*

Servicing Security Activity/SSO *[Signature]*

NATO Program Manager *[Signature]*

Restricted Data Program Manager *[Signature]*

SAP Program Manager *[Signature]*

Contract expiration date _____

Number of SCI billets Authorized: The CIA will approve SCI access for all JASON personnel supporting this contract.

Solicitation #W15P7T04RA202
Attachment 1

Release of Non-SCI Intelligence Information to DoD Contractors

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO #

CONTRACT EXPIRATION DATE

1. Requirements for access to non-SCI:
 - a. All intelligence material released to the contractor remains the property of the US Government and may be withdrawn at any time. Contractors must maintain accountability for all classified intelligence released into their custody.
 - b. The contractor must not reproduce intelligence material without the written permission of the originating agency through the Intelligence Support Office. If permission is granted, each copy shall be controlled in the same manner as the original.
 - c. The contractor must not destroy any intelligence material without advance approval or as specified by the contract monitor (CM). (EXCEPTION: Classified waste shall be destroyed as soon as practicable in accordance with the provisions of the Industrial Security Program).
 - d. The contractor must restrict access to only those individuals who possess the necessary security clearance and who are actually providing services under the contract with a valid need to know. Further dissemination to other contractors, subcontractors, other government agencies, private individuals or organizations is prohibited unless authorized in writing by the originating agency through the CM.
 - e. The contractor must ensure each employee having access to intelligence material is fully aware of the special security requirements for this material and shall maintain records in a manner that will permit the contractor to furnish, on demand, the names of individuals who have had access to this material in their custody.
 - f. Intelligence material must not be released to foreign nationals or immigrant aliens whether they are consultants, US contractors, or employees of the contractor and regardless of the level of their security clearance except with advance written permission from the originator. Requests for release to foreign nationals shall be initially forwarded to the contract monitor and shall include:

Solicitation #W15P7T04RA202

- (1) A copy of the proposed disclosure.
- (2) Full justification reflecting the benefits to US interests.
- (3) Name, nationality, particulars of clearance, and current access authorization of each proposed foreign national recipient.

g. Upon completion or termination of the classified contract, or sooner when the purpose of the release has been served, the contractor will return all classified intelligence (furnished or generated) to the source from which received unless retention or other disposition instructions (see DCID 611) are authorized in writing by the CM.

h. The contractor must designate an individual who is working on the contract as custodian. The designated custodian shall be responsible for receipting and accounting for all classified intelligence material received under this contract. This does not mean that the custodian must personally sign for all classified material. The inner wrapper of all classified material dispatched should be marked for the attention of a designated custodian and must not be opened by anyone not working directly on the contract.

i. Within 30 days after the final product is received and accepted by the procuring agency, classified intelligence materials released to or generated by the contractor, must be returned to the originating agency through the contract monitor unless written instructions authorizing destruction or retention are issued. Requests to retain material shall be directed to the CM for this contract in writing and must clearly indicate the justification for retention and identity of the specific document to be retained.

j. Classification, regrading or declassification markings of documentation produced by the contractor shall be consistent with that applied to the information or documentation from which the new document was prepared. If a compilation of information or a complete analysis of a subject appears to require a security classification other than that of the source documentation, the contractor shall assign the tentative security classification and request instructions from the contract monitor. Pending final determination, the material shall be safeguarded as required for its assigned or proposed classification, whichever is higher, until the classification is changed or otherwise verified.

2. Intelligence material carries special markings. The following is a list of the authorized control markings of intelligence material:

a. "Dissemination and Extraction of Information Controlled by Originator

Solicitation #W15P7T04RA202

(ORCON).” This marking is used, with a security classification, to enable a continuing knowledge and supervision by the originator of the use made of the information involved. This marking may be used on intelligence which clearly identifies, or would reasonably permit ready identification of an intelligence source or method which is particularly susceptible to countermeasures that would nullify or measurably reduce its effectiveness. This marking may not be used when an item or information will reasonably be protected by use of other markings specified herein, or by the application of the “need-to-know” principle and the safeguarding procedures of the security classification system.

b. “Authorization for Release to (Name of Country(ies)/International Organization.” The above is abbreviated “REL_____.” This marking must be used when it is necessary to identify classified intelligence material the US government originator has predetermined to be releasable or has been released through established foreign disclosure channels to the indicated country(ies) or organization.

3. The following procedures govern the use of control markings.

a. Any recipient desiring to use intelligence in a manner contrary to restrictions established by the control marking set forth above shall obtain the advance permission of the originating agency through the CM. Such permission applies only to the specific purposes agreed to by the originator and does not automatically apply to all recipients. Originators shall ensure that prompt consideration is given to recipients’ requests in these regards, with particular attention to reviewing and editing, if necessary, sanitized or paraphrased versions to derive a text suitable for release subject to lesser or no control markings.

b. The control marking authorized above shall be shown on the title page, front over, and other applicable pages of documents, incorporated in the text of electrical communications, shown on graphics, and associated (in full or abbreviated form) with data stored or processed in automatic data processing systems. The control marking also shall be indicated by parenthetical use of the marking abbreviations at the beginning or end of the appropriate portions. If the control marking applies to several or all portions, the document must be marked with a statement to this effect rather than marking each portion individually.

c. The control markings shall be individually assigned at the time of preparation of intelligence products and used in conjunction with security classifications and other marking specified by E.O. 12958 and its implementing security directives. The marking shall be carried forward to any new format in which the same information is incorporated including oral and visual presentations.

Solicitation #W15P7T04RA202

4. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirements and copies of the DD Form 254 and Statement of Work,

Solicitation #W15P7T04RA202
Attachment 2

RELEASE OF SENSITIVE COMPARTMENTED INFORMATION (SCI)
INTELLIGENCE INFORMATION TO US CONTRACTORS

ATTACHMENT TO DD FORM 254 FOR CONTRACT NO: #
SCI BILLETS AUTHORIZED:

CONTRACT EXPIRATION DATE:

1. Requirements for access to SCI:

- a. All SCI will be handled in accordance with special security requirements which will be furnished by the designated responsible special security office (SSO).
- b. SCI will not be released to contractor employees without specific release approval of the originator of the material as outlined in governing directives; based on prior approval and certification of "need-to-know" by the designated contractor.
- c. Names of contractor personnel requiring access to SCI will be submitted to the contract monitor (CM) for approval. (The contract monitor is identified on the reverse side of the DD Form 254.) Upon receipt of written approval from the CM, the company security officer will submit request(s) for special background investigations through the appropriate agency.
- d. Inquiries pertaining to classification guidance on SCI will be directed through the CSSO to the responsible CM as indicated on the DD Form 254.
- e. SCI furnished in support of this contract remains the property of the Department of Defense (DoD) department, agency, or command originator. Upon completion or cancellation of the contract, SCI furnished will be returned to the direct custody of the supporting SSO, at destroyed IAW instructions outlined by the CM.
- f. SCI will be stored and maintained only in properly accredited facilities at the contractor location.

2. The contract monitor (CM) will:

- a. Review the SCI product for contract applicability and determine that the product is

Solicitation #W15P7T04RA202

required by the contractor to complete contractual obligations. After the CM has reviewed the SCI product(s) for contract applicability and determined that the product is required by the contractor to complete obligations, the CM must request release from the originator through the Intelligence Division. Originator release authority is required on the product types below:

- (1) Documents bearing the control markings of ORCON, PROPIN.
- (2) GAMMA controlled documents.
- (3) Any NSA/SPECIAL marked product.
- (4) All categories as listed in DoD 5105.21-M-1, and appropriate DCIDS.
 - a. Prepare or review contractor billet/access requests to insure satisfactory justification (need-to-know) and completeness of required information.
 - b. Approve and coordinate visits by contractor employees when such visits are conducted as part of the contract effort.
 - c. Maintain records of all SCI material provided to the contractor in support of the contract effort. By 15 January (annually) provide the contractor, for inventory purposes, with a complete list of all documents transferred by contract number, organizational control number, copy number, and document title.
 - d. Determine dissemination of SCI studies or materials originated or developed by the contractor.
 - e. Within 30 days after completion of the contract, provide written disposition instructions for all SCI material furnished to, or generated by, the contractor with an information copy to the supporting SSO.
 - f. Review and forward all contractor requests to process SCI electronically to the accrediting SSO for coordination through appropriate SCI channels.
 - g. Request for release of intelligence material to a contractor must be prepared by the contract monitor (CM) and submitted to the Intelligence Support Office. This should be accomplished as soon as possible after the contract has been awarded. The request will be prepared and accompanied with a letter explaining the requirement and copies of the DD Form 254 and Statement of Work.