

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <small>(The requirements of the National Industrial Security Program Operating Manual apply to all security aspects of this effort)</small>				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)			3. THIS SPECIFICATION IS: (X and complete as applicable)				
a. PRIME CONTRACT NUMBER		<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases)		Date (YYMMDD) 010815		
b. SURCONTRACT NUMBER			b. REVISED (Supersede all previous specs)	Revision No.	Date (YYMMDD)		
<input checked="" type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER DASG60-01-R-0003	Due Date (YYMMDD)	c. FINAL (Complete item 5 in all cases)		Date (YYMMDD)		
4. IS THIS A FOLLOW-ON CONTRACT? [] YES [X] 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 [X] NO. If yes, complete the following: In response to the contractors request dated _____, retention of the identified classified material is authorized for a period of:							
6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)							
a. NAME, ADDRESS, AND ZIP		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)				
7. SUBCONTRACTOR							
a. NAME, ADDRESS, AND ZIP		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)				
8. ACTUAL PERFORMANCE							
a. LOCATION COLLATERAL ACCESS: Same as block 6 a. SCI ACCESS: See Block 13 - Remarks, SCI ADDENDUM		b. CAGE CODE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code)				
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT SYSTEMS ENGINEERING AND TECHNICAL ASSISTANCE CONTRACT							
10. THIS CONTRACT WILL REQUIRE ACCESS TO	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		YES		
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	<input checked="" type="checkbox"/>		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTORS FACILITY OR 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			e. PERFORM SERVICES ONLY		<input checked="" type="checkbox"/>		
(1) Sensitive Compartmented Information (SCI)	<input checked="" type="checkbox"/>		f. HAVE ACCESS TO US 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 THE 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 (Traditional)		<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"/>		
l. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>		l. OTHER (specify)				
m. OTHER (Specify) (UCI)	<input checked="" type="checkbox"/>		SEE BLOCK 13 REMARKS		<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 National Industrial Security Program Operating 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)

Deputy Commanding General, Acquisition
 U.S. Army Space and Missile Defense Command
 (SMDC-PA), P.O. Box 1500
 Huntsville, AL 35807-3801

PUBLIC RELEASE OF SCI NOT AUTHORIZED
 SEE BLOCK 13 - REMARKS, REGARDING PUBLIC RELEASE OF
 NMD & THAAD INFORMATION

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
 *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes, to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.*

- a. See Attached Pages (DD Form 254 Continuation Pages) for additional security guidance.
- b. See SCI Addendum.
- c. See the National Missile Defense (NMD) Addendum for additional security guidance and requirements for NMD related efforts.
- d. See THAAD Addendum for additional security guidance and requirements for THAAD related efforts.

Reference Item 12: Public Release.

a. NMD Public Release - Office of the Secretary of Defense, Ballistic Missile Defense Organization (External Affairs/ BMDO-EA), 7100 Defense Pentagon, Washington, DC 20301-7100.

b. THAAD Public Release - Commander, U.S. Army Aviation and Missile Command (AMSAM-PA), Redstone Arsenal, AL 35898.

REFERENCE BLOCK 10e(1): This contract requires access to Sensitive Compartmented Information (SCI). Requirements for the SCI portion of this contract are contained in the enclosed U.S. Army SCI Addendum to DD Form 254.


 William E. Cooper
 SCI Monitor

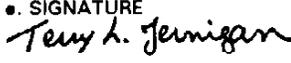
14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to NISPOM requirements, are established for this contract. YES NO
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is required.)

SCI & NON-SCI INTELLIGENCE INFORMATION, TEMPEST ANALYSIS AND OPSEC REQUIRED - SEE BLOCK 13, REMARKS
 SEE NMD AND THAAD ADDENDUMS 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 more space is needed.)* YES NO

BMDO/SCS is responsible for unclassified local area networks compliance inspections - See NMD Addendum

16. CLASSIFICATION 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.

<p>a. TYPED NAME OF CERTIFYING OFFICIAL</p> <p>TERRY L. JERNIGAN</p>	<p>b. TITLE</p> <p>Contracting Officer's Representative for Industrial Security</p>	<p>c. TELEPHONE (Include Area Code)</p> <p>(250) 955-1449</p>
<p>d. ADDRESS (Include Zip Code)</p> <p>Deputy Commanding General, Acquisition U.S. Army Space and Missile Defense Command (SMDC-IN-S), P.O. Box 1500 Huntsville, AL 35807-3801</p>		<p>17. REQUIRED DISTRIBUTION</p> <p>SMDC-IN-S SMDC-IM-PM JNI-ES (NMD P.O.) SFAE-AMD-THA</p> <p><input checked="" type="checkbox"/> a. CONTRACTOR</p> <p><input type="checkbox"/> b. SUBCONTRACTOR</p> <p><input checked="" type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME & SUBCONTRACTOR</p> <p><input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION</p> <p><input checked="" type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER</p> <p><input checked="" type="checkbox"/> f. OTHERS AS NECESSARY</p>
<p>e. SIGNATURE</p> <p></p>		<p>INSCOM, Contractor Support Element, (IASE-CSE), Bldg. 4554, Llewellyn Avenue, Fort Meade, MD 20755</p> <p>Def. Cour. Svc., Bldg. PT 830, Fort Meade, MD 20755-5370</p>

ITEM 13 Continuation

REFERENCE BLOCK 10a; Access to Communications Security (COMSEC) Information.

Contractor shall comply with the requirements of DOD 5220.22-M, DOD 5220.22-M-Sup1, NISPOM COMSEC Supplement, and all references contained therein. Contractor shall include COMSEC requirements to subcontractors, if applicable.

REFERENCE BLOCK 10e(2); Access to Intelligence Information (non-SCI)

The following guidelines concerning control and dissemination of intelligence information are based on DCID 1/7, 30 June 1998:

a. Intelligence information released under this contract or Request for Proposal (RFP) remains the property of the U.S. Government and may be withdrawn upon notice.

b. The contractor will maintain a record of all classified intelligence material released to your custody. Unclassified intelligence information will be treated as For Official Use Only (FOUO).

c. All reproductions of intelligence material will be classified, marked, and controlled in the same manner as original(s).

d. Prior to granting an employee access to intelligence materials, employees will be briefed on their obligation to comply with these procedures and will be debriefed when access to the material is terminated. A permanent list of all employees having had access to the intelligence materials during this contract will be maintained by the company and will be available for DSS inspection.

e. You will not release intelligence material to any activity, employee, or other person not directly engaged in providing services under this contract unless specific written authorization for such release is received from the Government Contacting Activity (GCA). This prohibition precludes release without authority to another contractor, Government agency, private individual, or organization unless a contractual relationship exists in support of this contract. Specific written authorization for such release will be received from Deputy Commanding General, Acquisition, U.S. Army Space and Missile Defense Command (SMDC-IN-S), P.O. Box 1500, Huntsville, AL 35807-3801.

f. The intelligence materials will not be released to foreign nations, non-U.S. citizens or U.S. citizens representing foreign entities except with specific written authorization from the GCA and USASMD C Foreign Disclosure Officer (FDO).

g. Intelligence materials released to you will be destroyed upon contract completion unless the GCA requests the return of the materials. A copy of the destruction certificate referencing

USASMDC control number will be mailed to Deputy Commanding General, Acquisition, U.S. Army Space and Missile Defense Command (SMDC-IN-S), P.O. Box 1500, Huntsville, AL 35807-3801, in order to remove contractor accountability from USASMDC records. However, returned intelligence information will be sent to the attention of the contract technical monitor, address identified in Section H of the contract. In the event the contract is extended or a new similar contract requiring the released data is initiated, it is the responsibility of the contract monitor to effect an extension or document transfer with the GCA.

h. All actions or inquiries concerning intelligence materials on this contract shall identify any **USASMDC control numbers**, if applicable, and shall be sent to the following address: Deputy Commanding General, Acquisition, U.S. Army Space and Missile Defense Command (SMDC-IN-S), P.O. Box 1500, Huntsville, AL 35807-3801.

REFERENCE BLOCK 10g; Access to NATO Information.

a. Upon expiration of the contract, all NATO material released to your company will be returned to the USASMDC NATO Subregistry, Deputy Commanding General, Acquisition, U.S. Army Space and Missile Defense Command (SMDC-IM-PM), P.O. Box 1500, Huntsville, AL 35807-3801.

b. NATO material released to your company will not be destroyed unless written authorization for such destruction is received from the USASMDC NATO Subregistry. A copy of the destruction certificate will be sent to the USASMDC NATO Subregistry, SMDC-IM-PM.

REFERENCE BLOCK 10h; Foreign Government Information.

a. Foreign government information is described as information provided to the U.S. by a foreign government or information produced by the U.S. as a result of a joint arrangement with a foreign government requiring that the information or arrangement be held in confidence.

b. Procedures for access to foreign government information in Chapter 10, Section 3 of the NISPOM apply.

c. Classified foreign government information will be afforded the same degree of protection as U.S. classified. Procedures in Chapter 10 and Appendix B of the NISPOM apply.

REFERENCE BLOCK 10j; For Official Use Only (FOUO) Information.

a. Contractors may disseminate "For Official Use Only" information to their employees and subcontractors who have a need for the information in connection with this contract.

b. Removal of the "For Official Use Only" marking can only be accomplished by the GCA. Request for public release of "For Official Use Only" shall be accomplished in accordance with item 12 of the DD Form 254-E.

c. "For Official Use Only" information shall be stored in locked receptacles such as file cabinets, desks, or bookcases.

When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection. During working hours, the 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.

d. "For Official Use Only" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail. Facsimile communications marked FOUO may be transmitted by nonsecure terminals with the FOUO marking intact between U.S. Department of Defense, and other U.S. Government agencies, and U.S. Government support contractors for official purposes.

e. 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.

f. Unauthorized disclosure of "For Official Use Only" information does not constitute a security violation but the GCA shall be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

REFERENCE BLOCK 11c; Receive and Generate Classified Material.

The below listed security classification guides apply to this specification. In the event that a security classification guide is superseded or replaced it is the responsibility of the Contract Monitor to provide such guides to the contractor.

a. U.S. Army Strategic Defense Command Ballistic Missile Defense (BMD) Classification Guide, 3 July 1989.

b. Airborne Surveillance Testbed (AST) Security Classification Guide, 29 January 1999.

c. Airborne Surveillance Testbed (AST) Topic 700 Attributes of Reentry Objects/Topic 900 Sensitive Programs, 29 January 1999.

d. U.S. Army Strategic Defense Command Survivability, Lethality, and Key Technologies (SLKT) Classification Guide, July 1992.

e. U.S. Army Space and Missile Defense Command Lethality Program Security Classification Guide, 27 December 1996.

f. Mark 12 and Mark 12A Reentry Vehicle (RV) Security Classification Guide, 15 April 1989.

g. High-Endoatmospheric Defense Interceptor (HEDI) Classification Guide, 28 March 1991.

h. Program Executive Office, Air and Missile Defense, Theater High Altitude Area Defense (THAAD) Project Classification Guide, 31 October 1997.

i. Concealment and Deception Technology (CDT) Security Classification Guide, October 1990.

- j. DoD Instruction #0-5210.85, 27 April 1993.
- k. Ballistic Missile Defense Organization Security Classification Guide, Directive Number 5230-M, 27 January 2000.
- l. SDIO/BMC3 Security Classification Guide, Including Information Control Procedures, May 1988.
- m. Joint United States (U.S.) - Government of Israel (GOI) Israeli Technology Experiment Program (ISTEP) Classification Guide, 17 May 1988.
- n. Minuteman Program Security Classification Guide, 30 July 1990.
- o. Peacekeeper Program Security Classification Guide, 30 January 1990.
- p. Pony Express Security Classification Guide, 31 July 1999.
- q. Mark 21 Reentry Vehicle (RV) Security Classification Guide, 27 April 1997.
- r. PATRIOT Air Defense Missile System Security Classification Guide, 27 August 1997.
- s. Red Tigress Security Classification Guide, 14 September 1995.
- t. Strategic Target Systems (STARS) Security Classification Guidance, 20 April 1989.
- u. ZODIAC BEAUCHAMP Security Classification Guide, May 1990.
- v. BMDO Countermeasures Program Security Classification Guide, March 1995.
- w. Brilliant Pebble (BP) Program, Pre-Full Scale Development (FSD) Flight Tests BP-1M and BP-TD Security Classification Guide, February 1993.
- x. Exoatmospheric Discrimination Experiment Security Classification Guide, 29 August 1990.
- y. Kinetic Energy Anti-Satellite (KE-ASAT) Initiative Security Classification Guide, 21 September 1998.
- z. Operational and Development Experiments Simulator (ODES) Security Classification Guide, 3 August 1998.
- aa. Joint DoD-DoE Radiation Hardened Microelectronics Classification Guide, January 1989.
- ab. BMDO Laser Radar Program Security Classification Guide, 5 May 1995.
- ac. Ground Based Surveillance and Tracking System (GSTS) Security Classification Guide, 15 May 1992.

ad. Joint Tactical Missile Defense System Security Classification Guide, February 1990.

ae. SDIO Command and Control (C2E) Security Classification Guide, 15 June 1992.

af. National Missile Defense (NMD) Security Classification Guide, July 1998.

ag. Target Reentry Vehicle Security Classification Guide, 8 November 1999.

ah. Additional classification guides will be provided under separate cover in anticipation of work that involves specific additional classification situations.

The marking to identify derivative source on classified documents generated shall cite the appropriate Security Classification Guide/s listed above, or otherwise shall cite the applicable derivative source material when classification is derived from source(s) other than the above security classification guides. All security markings shall be appropriately applied to comply with the NISPOM.

REFERENCE BLOCK 11f; Access to U.S. Classified Information Outside the U.S., Puerto Rico, U.S. Possessions and Trust Territories.

This contract may require your company to have access to classified information in an overseas area. The specific overseas area(s) will be provided by the Contract Monitor or the Contracting Officer. Classified information or materials will remain under the direct control of the U.S. government while in an overseas area unless prior approval is granted by this command. Release of classified information to a foreign entity will be accomplished in accordance with Chapter 10, NISPOM.

REFERENCE BLOCK 11h; Require a COMSEC Account.

The contractor will maintain a current listing of all COMSEC accountable equipment and/or material associated with this contract. A copy of this listing will be filed with the contract DD Form 254.

REFERENCE BLOCK 11j; Have OPSEC Requirements.

This contract requires the application of Operations Security (OPSEC). Contractors will follow the USASMDC SETAC Operations Security (OPSEC) Plan. This plan will be provided under separate cover.

REFERENCE BLOCK 11l;

a. Use Of Non-U.S. Citizens:

(1) Prior approval to use non-U.S. citizens on this contract must be obtained from the USASMDC Contracting Officer (CO) and USASMDC Foreign Disclosure Officer (FDO). However, if approval is granted, U.S. Export Laws still apply and the contractor must obtain required export licenses. When requesting

non-U.S. citizen access to the contract include the individual's full name, date and place of birth, social security account number and official status within the U.S.

(2) The contractor is not authorized to release any data to foreign nationals or foreign representatives without an approved export license.

(3) Sub-contracting with foreign industry is not allowed unless approved by the USASMDC CO and the USASMDC FDO. Foreign sub-contractors must agree that only citizens of their country or the U.S. will be allowed to perform on the contract. The U.S. Contractor is responsible for obtaining export licenses and providing the license number to the USASMDC CO and USASMDC FDO.

(4) The contractor is not authorized to release information, orally, visually, or documentary to anyone not associated with this contract.

b. Requirement for TEMPEST Analysis.

The contractor shall prepare a TEMPEST analysis using the guidelines of the National Security Telecommunications & Information System Security Instruction (NSTISSI) No. 7000, "TEMPEST Countermeasures for Facilities." The results of the TEMPEST analysis shall be forwarded to the below address. If TEMPEST countermeasures are required, you shall be notified of the specific TEMPEST countermeasures to be enacted. Unless further notified, no specific TEMPEST Countermeasures are required.

Deputy Commanding General, Acquisition
U.S. Army Space and Missile Defense Command
(SMDC-IN-S)
P.O. Box 1500
Huntsville, AL 35807-3801

c. All questions regarding security requirements indicated herein will be referred to the Contact Technical Monitor, if one is designated in Section H of the contract, or the Contracting Officer.

U.S. ARMY SCI ADDENDUM TO DD FORM 254

X (1) This contract requires access to Sensitive Compartmented Information (SCI). The Commander, U.S. Army Intelligence and Security Command (INSCOM), acting on behalf of the DA Deputy Chief of Staff for Intelligence (DCSINT), as the Cognizant Security Authority (CSA) for the U.S. 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:

- X DoD 5105.21-M-1, SCI Security Manual, Administrative Security.
- X DoD TS-5105.21-M-2, SCI Manual, COMINT Policy.
- X DoD TS-5105.21-M-3, TK Policy.
- NA DCID 1/21, Physical Security Standards for Construction of SCIFs.
- NA DIAM 50-4, DoD Intelligence Information System.
- NA DIAM 50-24, Security Policy for Using Communications Equipment in a SCIF.
- NA AR 380-19, Information System Security.
- X AR 380-28, DA Special Security System.
- NA AR 380-381, Special Access Programs (SAPs).
- X U.S. Army Handbook for SCI Contracts.
- NA Other

X (2) Contract Estimated Completion Date: _____.

X (3) The name, telephone number and address of the Contract Monitor (CM) for the SCI portion of this contract is: Mr. William E. Cooper, (256) 955-1451, U.S. Army Space and Missile Defense Command (SMDC-IN), P.O. Box 1500, Huntsville, AL 35807-3801.

CONTRACTOR SECURITY POC:

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

X (5) The contractor will submit a written request for SCI visit certifications through the CM for approval of the visit. The certification request must arrive at the appropriate Contract Support Detachment (CSD) at least ten (10) working days prior to the visit.

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

NA (7) Security Classification Guides or extracts (are attached) (will be provided under separate cover) by the User Agency.

NA (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 1/16, Dir., Central Intelligence Directive, DIAM 50-4, and AR 380-19. (Note: Check only if item (1) indicates that a requirement exists for SCI AIS processing.)

NA (9) This contract requires a contractor SCIF.

X (10) This contract requires ____ (SI) 20 (SI/TK) ____ (SI/TK/G) billets. (This is the total number of billets authorized for contract, to include subcontractor & task order billets. The exact number of billets per contract will be negotiated before contract award. This number will not exceed 20 billets per contract. Each nominee for SCI access will require a written justification to be submitted for approval to the government SCI monitor identified in paragraph (3) above.

X (11) The contractor will perform SCI work under this contract at the following locations: USASMDC, Huntsville, AL and other accredited SCIFs as identified by the Government SCI Monitor.

National Missile Defense (NMD) ADDENDUM TO DD FORM 254,
USASMDC SETA CONTRACT

This addendum, to include Annex A and Annex B thereto, identifies additional security guidance and requirements for NMD related efforts.

REFERENCES;

The contractor shall comply with the following references and all references contained therein:

- a. BMDO Directive 5230-M, Ballistic Missile Defense Program Security Classification Guide, January 27, 2000.
- b. National Missile Defense (NMD) Security Classification Guide, July 1998.
- c. Air Force Space Command Global Positioning System, System Operations Protect Guide, 1 August 1997.
- d. BMDO Directive 5200, BMDO Security Policy Directive, Current Version.
- e. DOD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs.
- f. DOD Directive 5200.1-M, Acquisition Systems Protection Programs, Current Version.

REFERENCE BLOCK 10j; For Official Use Only (FOUO) Information.

For Official Use Only Information provided under this contract shall be safeguarded as specified in Annex A to this addendum entitled, "For Official Use Only (BMD Program-Related) Guidelines." **THIS REQUIREMENT WILL BE IMPOSED ON ALL SUBCONTRACTS AS APPLICABLE.**

REFERENCE BLOCK 10k; Unclassified Controlled Information (UCI).

Unclassified Controlled Information (UCI) is not classified, but requires protective measures to prevent unofficial disclosure. This includes Ballistic Missile Defense (BMD) Program-Related Information concerning intentions, capabilities or activities that must be protected from loss, misuse, or unauthorized access to, or modification, in order to keep an adversary from gaining a significant military, economic, or technological advantage. (Contact Mr. Mike Burris, BMDO/NMD Security, (256) 313-9645, for any needed clarification regarding the definition of BMD Program Related Information).

- a. Electronic transmission of UCI (voice, facsimile, and data) shall be only over approved secure communications circuits. Non-secure communications circuits may transmit UCI only when secure communications circuits are not available to satisfy mission requirements.
- b. Unclassified BMD Program-Related material can be sent through normal mail or distribution channels used for UNCLASSIFIED information.

c. BMD Program-Related material marked as For Official Use Only and Unclassified BMD Program related material is destroyed as classified waste, or by any method that will prevent reconstruction.

THIS REQUIREMENT WILL BE IMPOSED ON ALL SUBCONTRACTS IF APPLICABLE.

REFERENCE BLOCK 111;

a. External Electronic Transmission of UCI.

External electronic transmission of Unclassified Controlled Information (voice, facsimile, and data) shall be only over approved secure communications circuits. Non-secure communications circuits may transmit Unclassified Controlled Information only when secure communications circuits are not available to satisfy mission requirements. This should be accomplished using NIST-validated or NSA-endorsed encryption. **THIS REQUIREMENT WILL BE IMPOSED ON ALL SUBCONTRACTS AS APPLICABLE.**

b. Unclassified LAN Processing.

Contractor's Unclassified LAN Processing Unclassified BMD Program-Related Information Requires:

(1) Compliance with the provisions of OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

(2) Access to unclassified BMD program information must be limited to U.S. citizens or persons where access does not constitute an export, unless the access is authorized by BMDO/SC; or in the case of technical data, as defined by the ITAR, the access is covered by TAA or other form of duly licensed export. This requirement does not apply to use of commercial off-the-shelf (COTS) equipment and services that do not have export limitations imposed by U.S. National Security and/or export/disclosure policy guidelines. LAN access to Unclassified BMD program related information must be limited to persons that have a minimum Secret level clearance; have been the subject of a favorable completed National Agency Check (NAC) or a more stringent personnel security investigation (access pending completion of NAC and final clearance determination is authorized), or contractor equivalent.

NOTE: Contractor equivalent includes various background checks such as those performed by employers during hiring process, including local and state law enforcement and agency check, degree confirmation checks, previous employment checks, and other forms of employee screening commonly used by Defense Contractors to screen prospective employees. Contractor will document basis for favorable adjudication when contractor equivalent option is used.

(3) Submission of an AISSP outlining procedures IAW OMB Circular A-130, reviewed and approved by BMDO/SC, prior to processing. (This requirement is N/A if an AISSP has been previously submitted and approved by BMDO/SC.) **THIS REQUIREMENT WILL BE IMPOSED ON ALL SUBCONTRACTS AS APPLICABLE.**

c. Publicly Accessible Internet Web Sites/BMDO Extranet:

(1) Contractor and subcontractor computer systems that provide public access via an internet web site will contain only BMD information that has been officially approved for public release.

(2) Contractors and subcontractors are authorized to connect to the BMDO extranet site, which contains unclassified BMD program related information.

d All questions regarding security requirements indicated herein will be referred to the Contact Technical Monitor, if one is designated in Section H of the contract, or the Contracting Officer.

REFERENCE BLOCK 12; Public Release.

a. Proposed public disclosure of unclassified information (to include internet web sites) relating to work under this contract shall be coordinated with the Contracting Officer's Representative (COR) and BMDO External Affairs (BMDO/EA) for review. Only information that has been favorably reviewed and authorized by the Office of the Assistant Secretary of Defense (Public Affairs) may be disclosed. Information developed after initial approval for public release must be submitted for review and further processing.

b. Contemplated visits by public media representatives in reference to this contract shall receive prior approval from the COR and BMDO External Affairs.

c. Critical technology subject to the provisions of DOD Directives 5230.24, "Distribution Statements on Technical Documents," and 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," shall be reviewed in accordance with established directives. Any request from a foreign government or representative thereof, including foreign contractors, for classified and/or unclassified information in reference to this contract shall be forwarded to the BMDO Office of Security for review and appropriate action.

REFERENCE BLOCK 14; Additional Security Requirements.

a. Compliance with security requirements imposed by documents generated in response to DOD Directive 5000.1, Defense Acquisition System; DOD Regulation 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs; and the Technology Protection Handbook, December 1999 will be required.

Compliance with OPSEC measures, if imposed by documents generated by BMDO/SC in response to DOD 5000.1 and 5000.2-R requirements, will be required. The OPSEC program will be IAW DOD 5205.2, Department of Defense Operations Security Program, current version. Program protection measures shall be applied and approved by BMDO/SC at ALL locations where Critical Program Information (CPI) is developed, produced, analyzed, maintained, transported, stored, tested, or used in training. Program Protection Program must be in compliance with DOD 5000.2-R, Acquisition Systems Protection Program and DOD Directive 5200.1-M, Acquisition Systems Protection Programs.

b. Letters of Instruction issued by BMDO to clarify or expound on any aspect of security will be included as part of this Contract Security Classification Specification. All Letters of Instruction issued by BMDO subsequent to the issuance of this Contract Security Classification Specification to clarify or expound on any aspect of security will be binding and will be attached to the next revision of this document. (See Annex B to this specification entitled "Letters of Instruction" for a listing.) Letters of instruction will remain in effect until superseded or removed in an update to this specification.

REFERENCE BLOCK 15; Inspections.

BMDO/SC will be responsible for accreditation and compliance inspections for Unclassified Local Area Network connectivity. BMDO/SC will be responsible for conducting Protection Assessment Reviews (PARs) in accordance with DOD Directive 5200.1-M, Acquisition Systems Protection Program, to ensure contractor compliance with this contract specification.

ANNEX A, NMD ADDENDUM TO DD FORM 254, USASMDC SETA CONTRACT

FOR OFFICIAL USE ONLY (BMD PROGRAM-RELATED) GUIDELINES
(THIS GUIDANCE ALSO PERTAINS TO PRIVACY ACT (PA) INFORMATION)

I. General.

a. For Official Use Only (FOUO) is official government information that does not meet requirements for classification but still requires protection. BMD Program-Related, Privacy Act (PA), as well as other information falls in this category.

b. Under certain conditions, BMD Program-Related information may be released to the public; however, it must be reviewed by BMD/EA, with the concurrence of the NMD Task Order Monitor prior to official release.

II. Identification Markings.

a. An unclassified document containing BMD Program-Related information, if marked FOUO, will be marked "For Official Use Only" on the outside 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). For convenience, all pages, even those that do not contain FOUO information may be marked in documents generated by an automated system.

b. Individual pages within a classified document that contain both FOUO and classified information will be marked at the top and bottom with the highest security classification of information appearing on the page. Individual portions/ paragraphs containing FOUO information but no classified information will be marked "FOUO".

c. Certain classified material on this contract may be downgraded to FOUO by the Declassification Authority. When classified material that is approved to be declassified to FOUO is used, extracted, reissued, transmitted and/or updated, it must be reviewed and appropriately marked.

III. Transmission/Dissemination/Reproduction.

a. Authorized contractors, consultants and grantees may transmit/disseminate BMD Program-Related information internally to each other, to DOD components and officials of DOD components who have a legitimate need for the information in connection with this contract. The following general guidelines apply:

1. Electronic transmission of Unclassified Controlled Information (UCI) (voice, facsimile, and data) shall be only over approved secure communications circuits. Non-secure communications circuits may transmit UCI only when secure

communications circuits are not available to satisfy mission requirements.

2. BMD Program-Related and PA information shall be transmitted over secure facsimile equipment.

3. BMD Program-Related information may be transmitted, processed and stored internally on Automated Information Systems (AIS), electronic mail and other similar systems or networks 1) when distribution is to an authorized recipient and 2) if the receiving system is protected by either physical isolation or a password protection system. Holders will not use general, broadcast or universal mail addresses to distribute BMD Program-Related and PA information. Discretionary access control measures may be used to preclude access to BMD Program-Related files by users who are authorized system users but who are not authorized access to BMD Program-Related and PA information. External transmission of BMD Program-Related and PA information shall be secured using NIST-validated or NSA-endorsed encryption.

4. Internet should be equated with "Public Access". Information must be reviewed and officially approved for public release by the Office of the Secretary of Defense, Ballistic Missile Defense Organization (External Affairs/BMDO-EA), 7100 Defense Pentagon, Washington, DC 20301-7100, before placing on electronic systems.

5. BMD Program-Related information may be sent via US Postal Service or commercial carrier as long as the shipping package is not marked as containing BMD Program-Related material.

6. Reproduction of BMD Program-Related and PA information may be accomplished on unclassified copiers within designated government or contractor reproduction areas.

IV. Storage. During working hours, BMD Program-Related and PA information shall be used in a manner that limits access by persons who do not have an official need for the information. During non-working hours and when internal building security is provided, BMD Program-Related material may be filed with other unclassified records in unlocked files or desks. When there is no internal building security, locked buildings or rooms provide adequate after-hours protection or the material can be stored in locked receptacles such as cabinets, desks, or bookcases.

V. Disposition.

a. When no longer needed, FOUO non-BMD Program-Related information will be disposed of in a manner to hinder reconstruction, e.g., by tearing each sheet into pieces and placing in a recycle or trash container or by initializing, degaussing or shredding magnetic media. BMD program-Related and

PA information will be disposed of as classified waste. If the contractor does not have the facilities for proper destruction of BMD program-Related and PA information (waste material), it may be returned to the BMDO office for proper disposition.

b. Removal of the FOUO or BMD Program-Related status can only be accomplished by the government originator. The BMDO COR will review and/or coordinate with proper authority the removal of FOUO or BMD Program-Related status for information in support of this contract.

VI. Unauthorized Disclosure. Government and contractor personnel must act to protect BMD Program-Related and PA information under their control from unauthorized disclosure. Government and contractor organizations must inform the NMD Task Order Monitor and BMDO/SC of any unauthorized disclosures of BMD Program-Related and PA information in support of this contract. Unauthorized disclosure, intentional disregard or gross negligence in the handling of BMD Program Related information does not constitute a reportable security violation. However, the responsible organization should investigate and, when substantiated, take appropriate disciplinary action. Unauthorized disclosure of FOUO information containing Privacy Act information may also result in civil or criminal sanctions.

ANNEX B, NMD ADDENDUM TO DD FORM 254, USASMDC SETA CONTRACT

LETTERS OF INSTRUCTION

Waiver of "Need-to-Know" Requirement for Visits to the Joint National Test Facility	BMDO/DSCO, 20 Jul '98
Authority for Subcontractors to Exchange Classified Information	BMDO/DSCO, 6 Jul 98
Disclosure of Critical Nuclear Weapons Design Information and Intelligence Information	BMDO/DSCO, 6 Jul 98
Technical Assistance Agreement	BMDO/DSC, 1 Oct 98
DOD Use of International Traffic-in-Arms Regulations Exemptions	DTSA, 29 May 97
Revised Marking Requirements for Foreign Government Information	BMDO/DSIS, 16 May 97
For Official Use Only (BMD Program Related) Guidelines	BMDO/DSCO, Undated
BMDO Directive 5200, BMDO Security Policy Directive	BMDO/DSC, Current Version
Visit Authorization Requests; Contract HQ0006-98-C-0003	BMDO/DCTD/LSI/99-129, Mar 25, 99
Classification of Data Pertaining to Commercial-Off-the-Shelf (COTS) NMD System Components	JN, 7 Dec 98
NMD Booster Verification Test Telemetry Security at Vandenberg AFB (VAFB)	BMDO/DSC, 26 May 99
Letter, COTS Booster Telemetry Data Classification	JN/I, undated
COMSEC Information Authorization under Contract HQ0006-98-C-0003	BMDO/DCTD/LSI/99-193, dtd 6/30/99
Upgraded Early Warning Radar Security Classification Guidance	BMDO/DCTD/LSI/99-0315, 10 Nov 99
ESC/NDWU SECRET Memorandum dtd May 15, 2000, Regarding Procedures for Protecting the Security of AFSPC PAVE PAWS Radars	CTN/LSI/00240, dated 8/3/00
NMD Security Classification Guidance for the GBR-P Effort under NMD LSI Contract HQ0003-98-C-0003	CTN/LSI/00-0299, dated 9/29/00
Approval for Contractor Use of Government Sources of Supply and NMD Security Classification Guidance for the GBR-P Effort, NMD Prime Contract HQ0006-01-C-0001	CTN/NMD/01003, dtd 1/3/01

** Contact Mr. Mike Burris, BMDO/NMD Security, (256) 313-9645, for copies of the above references.

Theater High Altitude Area Defense (THAAD) ADDENDUM TO
DD FORM 254, USASMDC SETA CONTRACT

This addendum identifies additional security guidance and requirements for THAAD related efforts.

REFERENCE BLOCK 10j; For Official Use Only (FOUO) Information.

a. Contractors may disseminate "For Official Use Only" information to their employees and subcontractors who have a need for the information in connection with this contract.

b. Removal of the "For Official Use Only" marking can only be accomplished by the Government Contracting Activity (GCA). Request for public release of "For Official Use Only" shall be accomplished in accordance with item 12 of the DD Form 254-E.

c. "For Official Use Only" information shall be stored in locked receptacles such as file cabinets, desks, or bookcases. When such internal security control is not exercised, locked buildings or rooms will provide adequate after-hours protection. During working hours, the 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.

d. "For Official Use Only" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail. Facsimile communications marked FOUO may be transmitted by non-secure terminals with the FOUO marking intact between U.S. Department of Defense, and other U.S. Government agencies, and U.S. Government support contractors for official purposes.

e. "For Official Use Only" information will not be transmitted via e-mail unless encrypted.

f. 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.

g. Unauthorized disclosure of "For Official Use Only" information does not constitute a security violation but the GCA shall be informed of any unauthorized disclosure. The unauthorized disclosure of FOUO information protected by the Privacy Act may result in criminal sanctions.

REFERENCE BLOCK 10j; Have OPSEC Requirements.

In addition to the USASMDC SETAC Operations Security (OPSEC) Plan, contractors supporting THAAD efforts shall follow the THAAD OPSEC Plan. A copy of this plan can be obtained from the THAAD Security Office, (256) 955-1763.

REFERENCE BLOCK 11i; Requirement for Program Protection.

The contractor must protect critical program information in hardcopy format, system software, and hardware components. The Critical Program Information (CPI) as identified in the THAAD

Program Protection Plan (PPP) are not authorized for release outside the THAAD channels without express consent of the THAAD Project Manager, or his authorized representative.