Headquarters, Department of the Army, G-2

DD FORM 254
Preparation Guide

FY-10

FOREWORD

Within The Department of Defense, Industrial Security is identified as the portion of information security concerned with the protection of classified information in the custody of U.S. industry. The purpose of the Industrial Security Program is to safeguard classified information that may be or has been released to current, prospective or former contractors.

The purpose of this guide is to provide guidance in the preparation of a DD Form 254, Contract Security Classification Specification. This guide contains step-by-step procedures for completing the DD Form 254. The instructions in this guide correspond to the numbered items on the form.

The intention of a DD Form 254 is to convey security requirements, classification guidance and provide handling procedures for classified material received and/or generated on a classified contract. The DD Form 254 is a resource for providing security requirements and classification guidance to a contractor. The DD Form 254 is a U.S. publication referenced in the DFAR and applied to contracts involving access to classified information by U.S. contractors. If the contract is with non-US Industry (foreign governments, cleared foreign companies or international organizations) additional guidance is on a case-by-case basis. The Industrial Security Implementing Agreement (to the General Security of Military Information Agreement) is the overarching authority for the bilateral protection of classified information with foreign governments. Any guidance provided to contractors to explain protection requirements for classified information exchanged under bilateral agreements must be conveyed through security contract clauses, and not a DD Form 254.

NOTE: U.S. Industry is any company, educational institution, commercial association/organization or other entity established and operating as a legitimate business or enterprise and granted a Facility Security Clearance (FCL) by a cognizant security agency (CSA).

Any misconduct/wrongdoing of a contractor, modification to the contract or changes to the company ownership status, which could have an adverse impact upon national security, the Army program and/or information, must be reported immediately to the Contract Officer (KO) or a Contract Officer Designated Representative. (Note: For purposes of this handbook, the term Contract Officer (KO) is used inclusively for the terms: Contracting Officer Representative (COR), Alternate COR (ACOR) or Contracting Officer Technical Representative (COTR)). The KO must be notified on all contract matters through the COR/ACOR/COTR.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION:

The Federal Acquisition Regulation (FAR) requires that a DD Form 254, Contract Security Classification Specification, be integrated in each classified contract. The DD Form 254 provides the contractor (or a subcontractor) security requirements and the classification guidance that is necessary to execute a classified contract. This handbook has been prepared from the Defense Security Service (DSS) guide, Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulations Supplement (DFARS), Army Federal Acquisition Regulations Supplement (AFARS), and National Industrial Security Program Operating Manual (NISPOM).

The Security Agreement (DD Form 441), executed between the government and all cleared facilities under the NISP, obligates the Government to provide the contractor appropriate classification guidance for the protection of the classified information, furnished to or generated by, the contractor in the performance of a classified contract. The Government fulfills this obligation by incorporating a "Security Requirements Clause" ("clause") and a DD Form 254 in each classified contract. The "clause" identifies the contract as a "classified contract" and the DD Form 254 provides classification guidance and the specific security requirements.

The DD Form 254 is a contractual specification. It is as important as any other specification in a contract. It is the vehicle that provides the contractor with the security classification guidance necessary for the classified information to be received and generated under the contract. It also identifies the level and specific types of classified information authorized on the contract. It was developed as a contractual document to capture in one place the security requirements for a classified contract. By checking the blocks for the preprinted items on the DD Form 254, the Contracting Office (KO), Contracting Officer Representative (COR)/Contract Monitor (CM) provides the contractor with a brief summary of the security requirements that apply to the contract.

The key personnel in the preparation of the DD Form 254 are the program and Industrial Security Specialist (ISS), technical/subject matter expert personnel, and contracting personnel. The program and ISS recognizes the security requirements that the contractor will need to follow. The technical/subject matter expert personnel understand what information or equipment in the program requires protection, and the technical aspects of the requirements, the KO must ensure the contractor complies with the DD Form 254 and any special clauses into the contract.

The DD Form 254 is required to be reviewed every two years. The program and ISS should conduct this review in coordination with the program manager of the requiring activity and KO to ensure that existing security requirements are consistent with the contract requirements.

If the review is performed and no changes are required, the program and ISS will provide the KO with a copy of the review. The KO will then send to the contractor, in writing, notification that the DD Form 254 remains valid until the next review or a change occurs in the program.

If the review is performed and changes are required the program and ISS must provide the KO with a revised copy. The KO will then prepare a bi-lateral modification to the contract incorporating the new DD Form 254.

The Defense Security Service (DSS) is designated by DoD Directive 5220.22, National Industrial Security Program (NISP), as the Cognizant Security Office (CSO) to administer industrial security on behalf of the Cognizant Security Agency (CSA). The CSAs are: the Department of Defense (DoD), Department of Energy (DOE), Central Intelligence Agency (CIA), and the Nuclear Regulatory Commission (NRC). The designation of DSS as the CSO for the Department of Defense does not relieve the Government Contracting Activity (GCA) of the responsibility to protect and safeguard classified information disclosed to or generated by contractors under the NISP or from visiting the cleared contractor to review the security aspects/requirements of the contract.

Revisions to the DD Form 254 will be completed whenever the security guidance or pertinent information changes, when a change in mission occurs impacting the contract, when a contract is modified or an option year is utilized, to ensure security requirements remain current and relevant throughout the contract lifecycle. This includes contractor address changes if they are performing classified work at their facility.

CHAPTER 2

POINTS OF CONTACT:

* HQDA, G-2
Industrial Security
Lisa Gearhart
703-601-1565

Or

HQDA, G-2
Industrial Security
Pamela Y. Spilman
703-601-1567

Mailing Address: HQDA, G-2
ATTN: DAMI-CDS
1000 Army Pentagon RM 2D350
Washington, DC 20310-1000

Facsimile number: 703-601-0733

E-Mail Address: Lisa.A.Gearhart@us.army.mil
Pamela.Spilman@us.army.mil

* Defense Security Services

Mailing Address: Defense Security Service
1340 Braddock Place
Alexandria, VA 22314

Telephone number: 1-888-282-7682

Website: www.dss.mil

* U.S. Army Intelligence and Security Command (INSCOM)/Contractor Support Element (For all Army SCI contracts)

Mailing Address
United States Army Intelligence and Security Command
Contractor Support Element (CSE)
4552 Pike Road, MS 5820
Fort Mead, MD 20755-5820

Facsimile number: 301-677-2901

E-Mail Address: cseoperations@mi.army.mil

* Technology Management Office
(For SAP contracts)

Mailing Address
Office of Chief of Staff of the Army
ATTN: Technology Management Office, DACS-ZDV-TMO
Attn: D. Scott Magnino, Security Manager
200 Army Pentagon, RM 2A528
Washington, DC 20310-0200

Telephone number: 703-695-4056
Facsimile number: 703- 697-4009

E-Mail Address: scottmagnino@hqda.army.mil

CHAPTER 3

Pre-Award Considerations

Before the KO or prime contractor issues a solicitation for a classified contract, a determination should be made as to whether or not access to classified information is required during the solicitation process.

If access to classified information is not required during the solicitation process, prospective contractors do not have to possess facility clearances to bid on the solicitation. However, the successful bidder must have a facility clearance to perform on the contract. The contracting team should make every effort to develop a solicitation package that does not require access to classified information. The solicitation DD Form 254 will be marked "For Planning Purposes Only" and provided to the supporting KO for review and incorporation into the requirements package. The preliminary DD Form 254 includes the what, why, when, and where for a contractor that will need classified information or access to classified information. The contractor should staff any changes to the security requirements through the program, COR/CM if one has been appointed, and ISS and back to the KO for incorporation into the solicitation.

If access to classified information is required during the solicitation process, all prospective contractors must possess the appropriate facility clearance and safeguarding capability in order to access the classified information within the solicitation package. If a reading room is provided by the Army to review the classified information for the solicitation, then the contractor's clearance eligibility must be verified prior to the review. To determine the current clearance status of prospective contractors, contact the DSS Central Verification Activity at 1-888-282-7682 or log on to the DSS web site (www.dss.mil) and follow the instructions. Prior to calling DSS' Central Verification Activity, you will need the contractor's Commercial and Government Entity (CAGE) code.

If any of the prospective contractors do not have the appropriate facility clearance, contact DSS and furnish, in writing, the information needed to sponsor the clearance. See the DSS website for additional sponsorship guidance:
http://www.dss.mil/isp/fac_clear/fac_clear.html.

Companies in the process of obtaining a facility clearance, or reporting any changes regarding the company information, will use the DSS Electronic Facility Clearance (e-FCL) online application to submit their documents to DSS. Contact the DSS Facility Clearance Branch at occ.facilities@dss.mil or go to the link above for additional guidance on facility clearances.

CHAPTER 4

INSTRUCTIONS:

Item 1. Clearance and Safeguarding.

1a. Facility Clearance Required: Insert the highest level of facility clearance required for the contractor to perform on the contract. Only one of three classification levels should be listed in this field: Confidential, Secret or Top Secret. The contractor must have a valid Facility Clearance at least as high as the classification indicated in this item. It is critical that the correct security level is established. Setting the security level too high may create undue costs and delay contract award.

(1) Do not cite special categories of classified such as Restricted Data, COMSEC, SCI, etc.

(2) Contractors must meet the facility clearance and safeguarding requirements of the DD Form 254. To verify the contractor's facility clearance and safeguarding capability, contact the DSS Central Verification Activity at 1-888-282-7682 or log on to the DSS web site (www.dss.mil) find the application tab in the upper right-hand corner, click on ISFD, then follow the instructions to either login or request access.

1b. Level of Safeguarding Required: Insert the highest level of safeguarding capability required for the contractor to perform on the contract. Safeguarding refers to the ability to store and/or generate classified materials at the contractor facility.

(1) If the contractor is working in the contractor facility the classification level may not be higher than Item 1a.

(2) If the contractor will NOT possess or store classified information at the contractor's facility, enter "Not Applicable" or "None." (If this is the case, Item 11a. must be marked "YES" and 11b and 11d must be marked "NO"). Block 8 "Actual Performance" will indicate the location where the classified work will be accomplished. If classified work will occur at multiple locations mark "multiple locations" in Block 8a and list the locations in Block 13 or an attached Appendix, as applicable.

DEPARTMENT OF DEFENSE **CONTRACT SECURITY CLASSIFICATION SPECIFICATION** *(The requirements of the DoD Industrial Security Manual apply to all aspects of this effort)*	**1. CLEARANCE AND SAFEGUARDING** a. FACILITY CLEARANCE REQUIRED b. LEVEL OF SAFEGUARDING REQUIRED

Item 2. This Specification is for:

Information for Blocks 2a and 2c are obtained from the government KO. Block 2a is completed upon contract award. Block 2b is completed by the contractor when a subcontract is awarded. Block 2c is completed prior to the release of the solicitation. Insert an "X" into the appropriate box. Although information may be entered into more than one box, only one "X" should appear in item 2 (a, b or c) depending what phase the acquisition is in.

2a. Prime Contract Number: Used when the KO issues the contract to the Prime Contractor. The contracting activity enters the contract number upon award.

2b. Subcontract Number: Used when there is a Prime Contractor/Subcontractor relationship. The contractor issuing the subcontract enters the subcontract number. The prime contract number must also be entered in 2a. Government agencies do not process DD Form 254s for subcontractors.

2c. Solicitation or other number: Used for an RFP, RFQ, IFB, or other solicitation, regardless of whether or not the bid package will contain classified information. The contracting activity enters the solicitation number and the date by which bids are due.

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*		
☐	a. PRIME CONTRACT NUMBER	
☐	b. SUBCONTRACT NUMBER	
☐	c. SOLICITATION OR OTHER NUMBER	Due Date *(YYYYMMDD)*

Item 3. This Specification Is:

Insert an "X" into the appropriate box. Although information may be entered in more than one box, only one "X" should appear in Item 3.

3a. Original

Original DD Form 254 is issued:

(1) For a solicitation for a classified contract, whether or not the actual bid package contains classified information.

(2) Upon the award of a classified contract

(3) Upon the award of a classified subcontract

The date of issuance is entered by the KO or prime contractor for subcontractors.

The 'Original date' refers to the release date of the DD Form 254. This date will not change over the period of the contract.

3b. Revised DD Form 254

(1) Revisions to the DD Form 254 will be completed whenever the security guidance or pertinent information changes, when a change in mission occurs impacting the contract, when a contract is modified or an option year is utilized, to ensure security requirements remain current and relevant throughout the contract lifecycle. Give a sequential number to each revision and enter the date of the revised DD Form 254.

(2) Enter the date of the original DD Form 254 in 3a.

Revised DD Form 254s should be numbered sequentially starting with "1". A revised DD Form 254 is generated any time there is a change to the security requirements or to the classification guidance. A revised DD Form 254 is also required if the contractor has safeguarding requirements and there is a change of location of their facility. Revised DD Form 254s should be prepared and reviewed by the program and ISS and the KO. It is recommended that all the reviewers sign as certifying officials in block 13 (see Item 13 for more details on signatures). A revised DD Form 254 MUST be incorporated into the contract by modification.

3c. Final DD Form 254

(1) When a contract is closed out, the contractor may request additional retention authority that may result in a Final DD Form 254. If an extension of retention authority is approved by the KO, a final DD Form 254 may be issued to reflect this approval. (See NISPOM Chapter 5, Section 7 for more information on disposition and retention.)

(2) Enter the date the final DD Form 254 is issued. Complete Item 5.

(3) Enter the date of the original DD Form 254 in 3a.

A final DD Form 254 is ONLY used to authorize retention of classified materials beyond 2 years from the end of the contract as allowed by the NISPOM. If section 3c is marked "YES", Line 5 must also be completed.

NOTE: Item 5 is always marked "YES" when a final DD Form 254 is issued. Additional retention authorization may also be granted through email or a letter to the contractor.

3. THIS SPECIFICATION IS: ***(X and complete as applicable)***			
☐	a. ORIGINAL *(Complete date in all cases)*		Date *(YYYYMMDD)*
☐	b. REVISED *(Supersedes all previous specs)*	Revision No.	Date *(YYYYMMDD)*
☐	c. FINAL *(Complete Item 5 in all cases)*		Date *(YYYYMMDD)*

Item 4. A Follow-On Contract. If this contract is a follow-on to an existing contract complete this block.

A Follow-On Contract is a contract awarded to the same contractor or subcontractor for the same item or services as a preceding contract. When this occurs, mark "YES" and enter the preceding contract number in the space provided. This item authorizes the contractor or subcontractor to transfer material/information received or generated under the preceding contract to the new contract. The transferred material/information will be reflected in Item 13. If unsure, check with the KO they will have this information. During a competitive contract action this information may not be known until the contract is awarded.

Enter the following statement in Item 13:

> **Ref 4:** The classified portion of work has been completed on the contract cited in this block. The processing of classified will no longer be done under this contract. All classified material/ information associated with this contract is authorized to be transferred to the contract number cited in block 2a.

4. IS THIS A FOLLOW-ON CONTRACT?	☐ YES	☐ NO. If Yes complete the following
Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract		

Item 5. Final DD Form 254

If this is a FINAL DD Form 254, mark "YES". Enter the date of the contractor's request for retention and the authorized period of retention in the spaces provided. If this is not a FINAL DD Form 254, mark "NO." The KO will inform the program and ISS of pending contract closure. This notification will prompt the program and ISS to provide the KO with close out/destruction instructions. Upon contractor notification to the KO that all classified information under the contract has been removed, destroyed, or designated for retention in accordance with the instructions provided, the Final DD Form 254 is prepared.

A final DD Form 254 is used only if the contractor requests the right to retain any project related documents beyond NISPOM permitted timeframe (See Item 3c.). Permission for extended retention of contract material/information must be requested in writing from the KO. It is recommended that the contractor maintains a copy of the formal request until retention authorization is received from the KO. The KO will determine if the designated material/information should be destroyed, returned or retained by the contractor.

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 identified classified material is authorized for the period of _____ .

Item 6. Contractor:

Used when the KO issues guidance to a prime contractor. Enter the required information once the clearance information has been verified and the contractor meets the requirement of the contract:

6a. Name and address of the contractor

6b. Contractor's CAGE code

The CAGE code is a Government issued unique identifier required for all companies who do business with the Government. CAGE codes can be verified through the Defense Logistics Information Service website at http://www.dlis.dla.mil/cage_welcome.asp. It is important to note that not all facilities with CAGE codes are cleared facilities. To verify a contractor's facility clearance see item 1a.

6c. The appropriate CSO and address

The local DSS Cognizant Security Office (CSO) and Field office locations can be found by going to https://www.dss.mil/GW/ShowBinary/DSS/isp/dss_oper_loc.html

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*		
a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

Item 7. Subcontractor:

The prime contractor will fill in this information and provide the DD Form 254 to the KO upon determination that the subcontract meets the security requirements;

7a. Name and address of the subcontractor

7b. The subcontractor's CAGE code

7c. The appropriate CSO and address

NOTE:

All DD Form 254s prepared for subcontracts involving access to SCI must be forwarded to the Contract Monitor for approval. Upon Contract Monitor approval, forward the DD Form 254 to Contractor Support Element (CSE) for review and concurrence prior to award of the subcontract.

All DD Form 254s prepared for subcontracts involving access to classified material must be forwarded to the KO (KO/COR/CM) and supporting ISS for review prior to award of the subcontract and attached to the prime contract.

7. SUBCONTRACTOR		
a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

Item 8. Actual Performance:

List **ALL** locations where classified performance is required under the contract (i.e. contractor, subcontractor, and Government facilities).

(1) If the place of performance is the same as 6a (or 7a), either enter the facility's name or enter "Same as Item 6a (or 7a) in block 8a. If the place of performance is different from 6a (or 7a), include the facility name, address and CAGE code.

(2) If there is more than one place of performance, enter "multiple locations - see Item 13 (or Attachment xxx)" in item 8a, and identify each performance location accordingly.

(3) Performance of a contract in Government facilities should be explained in Item 13. The location will be placed in item 8a. (e.g. Pentagon).

8a. Facility name and address

8b. The CAGE code of the facility where the work will be performed.

8c. The appropriate CSO and address:

8. ACTUAL PERFORMANCE		
a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

Item 9. General Identification of this Procurement

Enter a concise and unclassified description of the procurement action. Some examples could be research, development, production, study or services, etc. **Do not** use classified information such as project names or descriptive information. Keep this field short but informative.

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Item 10. This Contract Will Require Access To:

Mark all items "YES" or "NO," as appropriate to the requirements of the contract. (Coordinate with the appropriate program and other security offices to ensure the proper types of access are imposed on the contractor or subcontractor.) An explanation of each item follows.

IMPORTANT: These are access requirements for the contractor and their employees. It does not refer to safeguarding.

10a. Communications Security: COMSEC information includes accountable or non-accountable COMSEC information and controlled cryptographic items (CCI).

(1) If accountable COMSEC material is involved, the contractor must have a COMSEC account and item 11h must be marked "YES."

NOTE: COMSEC custodians are DA civilians or military members. Contractors are considered hand receipt holders. See AR 380-40 for further guidance on COMSEC.

(2) Prior approval from the KO is required in order for a prime contractor to grant COMSEC access to a subcontractor. The prime contractor must notify the NSA Central Office of Record before negotiating or awarding subcontracts.

When this item is marked "YES", enter the following statement in Item 13:

> **Ref 10a:** Classified COMSEC material is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. COMSEC access shall be IAW DoD 5220.22-M and AR 380-40. When access is required at Government facilities, contractor personnel will adhere to COMSEC rules and regulations as mandated by Command policy and procedures. Written concurrence of the KO is required prior to subcontracting.

10b. Restricted Data: Mark "YES" if access to RESTRICTED DATA information is required under the contract.

(1) 10b must be marked "YES" if item 10c is marked "YES."

When this item is marked "YES", enter the following statement in Item 13:

> **Ref 10b:** Restricted Data Information is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting.

10c. Critical Nuclear Weapon Design Information (CNWDI): Mark "YES" if access to CNWDI is required under the contract.

(1) KO approval is required prior to granting CNWDI access to a subcontractor. Special briefings and procedures are also required. Access to CNWDI requires a final U.S. Government clearance at that appropriate level.

(2) 10c must be marked "YES" if item 10b is marked "YES."

When this item is marked "YES", enter the following statement in Item 13:

Ref 10c: CNWDI Information is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting.

10d. Formerly Restricted Data (FRD): Mark "YES" if access to FRD is required.

Enter the following statement in Item 13:

Ref 10d: The contractor is permitted access to Formerly Restricted Data (FRD) in the performance of this contract. Access to FRD requires a final U.S. Government clearance at the appropriate level. Written concurrence of the KO is required prior to subcontracting.

NOTE: Access to FORMERLY RESTRICTED DATA requires a final U.S. Government Clearance at the appropriate level.

10e. Intelligence Information: The Director of National Intelligence (DNI) has jurisdiction and control of intelligence information. If the contract requires access to intelligence information, the KO is responsible for ensuring that the additional security requirements outlined in the DNI Directives are incorporated in the guidance provided to the contractor. If the contract requires Sensitive Compartmented Information (SCI) access, a SCI Addendum is required and **MUST** be coordinated with the Contractor Support Element (CSE). SCI is very expensive for the contractor to maintain. This block should not be marked unless there is a current SCI requirement.

If access to SCI is required:

(1) Mark 10e(1) "YES."

(2) Mark Items 14 and 15 "YES."

If access to non-SCI is required:

(1) Mark 10e(2) "YES."

(2) Mark Item 14 “YES”

(3) Mark Item 15 “NO.”

If access to SCI and non-SCI is required:

(1) Mark 10e(1) and 10e(2) “YES.”

(2) Mark Item 14 “YES.”

(3) Mark Item 15 as appropriate

Prior approval by the KO is required before a subcontract involving access to Intelligence Information can be issued. Access to Intelligence information requires a U.S. Government clearance at the appropriate level.

When item 10e(1) is marked “YES”, enter the following statement in Item 13:

Ref 10e(1): SCI Access required. No public release of information authorized, public disclosure or confirmation of any subject related to the support contract is not authorized without first obtaining written approval from the KO.

When item 10e(2) is marked “YES”, enter the following statement in Item 13:

Ref 10e(2): Non-SCI Information is not releasable to contractor employees who have not received a clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting. Access to Intelligence information required for performance.

NOTE: DSS does not conduct security reviews for Sensitive Compartmented Information (SCI) but is still responsible for security reviews involving Non-SCI (collateral classified information) in the possession of a contractor or subcontractor.

10f. Special Access Information: Special Access Programs (SAP) imposes security requirements on the contractor that exceed the NISPOM. When SAP information is involved, the cognizant SAP security office is responsible for providing the contractor with the additional security requirements needed to ensure adequate protection of SAP information.

If SAP requirements are imposed on the contractor:

(1) Mark 10f “YES.”

(2) Mark Item 14 “YES.”

(3) Complete Item 15 as appropriate. (Some SAPs qualify as carve-outs, but not all SAPs are carve-outs – see AR 380-381 for additional guidance.)

If a SAP subcontract is awarded, the prime contractor is responsible to incorporate the additional security requirements in the subcontract. The Program Manager must grant authorization for release of SAP information to the subcontractor prior to issuance of any SAP subcontract.

The additional requirements can be included in the contract document itself or Item 13 only if the requirements are unclassified IAW the program security classification guide. Classified requirements shall be included in a separate SAP Addendum. (Block 13 should reference a Program Security Guide and Program Classification Guide. The guides should not be older than 5 years. If the Program Security Guide and Program Classification Guide are older or approaching their 5 year threshold, request updated guides from the cognizant SAP security office.)

A SAP Addendum is required for all contracts that require SAP access. Additional clarification should be addressed in either Item 13 or the SAP Addendum and are as follows:

- What information makes the hardware/services classified?
- Will hardware/data being generated require classification? At what stage in the production will it become classified?

Be sure to:

- identify the specific information to be classified
- provide appropriate downgrading or declassification instructions, and
- provide any special instructions, explanations, comments or statements necessary to clarify other items identified in the DD Form 254.

Enter the applicable statement in Item 13:

Ref 10f: Discussion, storage, or processing of SAP information associated with this contract will be conducted in facilities specifically accredited by the Army SAPCO (or designee), or equivalent component-level SAPCO. Contact the appropriate servicing SAPCO for approved SAP facilities locations. SAP activities are governed by Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement, 1 APR 04, and applicable program security classification and procedures guides. Component-managed SAPFs and SAP Temporary Secure Working Areas (TSWA) are governed by JAFAN 6/9. Access to SAP information requires employees undergo additional personnel security screening and meet the SAP access standards delineated in the applicable DoD directives and policies. SAP inspections and security oversight while in component facilities

are under the cognizance of the SAPCO, as appropriate. Additional SAP security requirements may apply at alternate locations/facilities based on service/component Command requirements. The KO for these locations/facilities will provide specific guidance as required. SAP inspections conducted at contractor facilities are under the security oversight of the Defense Security Service (DSS) unless officially relieved of their oversight responsibilities.

10g. NATO Information: Mark "YES" if the contract requires access to information or documents belonging to the NATO. The prime contractor must receive approval from the KO to grant NATO access to a subcontractor.

Enter the following statement in Item 13:

Ref 10g: Personnel not assigned to a NATO staff position, but requiring access to NATO classified information, NATO COSMIC, NATO Secret or access to the NATO accredited SIPRNET terminals, must possess the equivalent FINAL or Interim U.S. Security Clearance based upon the appropriate personnel security investigation required. Personnel with access to NATO ATOMAL information must have the appropriate level FINAL U.S. Security Clearance. The government program/project manager is the designated representative that will ensure the contractor security manager and concerned employees are NATO briefed prior to access being granted. The contractor will maintain strict compliance in regards to NATO information IAW NISPOM Ch 10, Section 7. Prior approval from the KO is required for subcontracting.

Note: If the contractor does not require access to NATO information, requires access to the SIPRNET, mark 10g "No" but mark 10k "Yes" (SIPRNET access) and add the statement below in item 13 that the contractor requires access to the SIPRNET and a NATO awareness brief is required. The SIPRNET contains NATO information and a NATO awareness briefing is required for everyone who needs access to the SIPRNET. The purpose of providing a NATO awareness briefing is to inform personnel how to protect NATO information in the event they come across it while on the SIPRNET. See 10k below for additional information.

10h. Foreign Government Information (FGI): This is classified information that is provided to the U.S. Government by a foreign government(s); an international organization, or any element thereof. **This does not include NATO information**. Mark "YES" if applicable. The prime contractor must receive approval from the KO to grant access to a subcontractor.

Enter the following statement in Item 13:

> **Ref 10h:** Foreign Government Information (FGI) is not releasable to contractor employees who have not received a FINAL clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting.

10i. Limited Dissemination Information (LIMDIS): This is no longer a valid program. New documents or contracts will not reflect this caveat. Until the DD Form 254 is revised, this block should be marked "NO."

10j. For Official Use Only Information: This item is linked directly to the Freedom of Information Act (FOIA) and the appropriate exemptions are in accordance with 5 U.S.C.§ 552(b), and should only be marked if the information the contract company will be accessing is protected under the FOIA. The NISPOM does not provide guidance concerning FOUO; the DD Form 254 must provide guidance on protection procedures in Item 13.

Enter the following statement in Item 13:

> **Ref 10j:** For Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD 5200.1-R, Appendix 3 (attached).

Sample Attachment

FOUO DD FORM 254 ATTACHMENT

Contract Number:

PROTECTING "FOR OFFICIAL USE ONLY" (FOUO) INFORMATION

1. GENERAL:

a. The "For Official Use Only" (FOUO) 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 is used on official government information that may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (FOIA).

b. 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 instruction received from such agencies.

c. Use of the above markings does not mean that the information cannot be released to the public under FOIA, only that the Government must review the information prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions thereof.

2. 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).

b. Within a classified document, an individual page that contains both FOUO and classified information will be marked at the top and bottom with the highest security classification of information 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 the "For Official Use Only" status is terminated, all known holders will be notified to the extent practical.

3. 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. Contractors must ensure employees and subcontractors are aware of the special handling instructions detailed below.

4. 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 nonworking 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 nonworking hours. When such internal security control is not exercised, locked buildings or rooms will provide adequate after- hours protection or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases.

5. TRANSMISSION: "For Official Use Only" information may be sent via first-class mail or parcel post. Bulky shipments may be sent by fourth-class mail. DoD components, officials of DoD components, and authorized DoD contractors, consultants, and grantees send FOUO information to each other to conduct official DoD business. Tell recipients the status of such information, and send the material in a way that prevents unauthorized public disclosure. Make sure documents that transmit FOUO material call attention to any FOUO attachments. Normally, you may send FOUO records over facsimile equipment. To prevent unauthorized disclosure, consider attaching special cover sheets, the location of sending and receiving machines, and whether authorized personnel are around to receive FOUO information. FOUO information may be passed to officials in other departments and agencies of the executive and judicial branches to fulfill a government function. Mark the records "For Official Use Only" and tell the recipient the information is exempt from public disclosure under the FOIA and requires special handling.

6. DISPOSITION: When no longer needed, FOUO information must be shredded.

7. 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 and disciplinary action may be taken against those responsible.

10k. Other: This item may be used for any other information not included in items 10a through 10j. Specify the type of information and include any additional remarks in item 13.

If the requirement is for SIPRnet only, the following statement must also appear in block 13:

> **Ref 10k:** Secret Internet Protocol Network (SIPRNET) access required. The contractor shall not access, download or further disseminate any special access data (i.e. intelligence, NATO, COMSEC, etc.) outside the execution of the defined contract requirements and without the guidance and written

permission of the KO. In the event that any special access is required, the KO must modify the requirements for the DD Form 254.

Note: Once the KO has modified the requirements for the DD Form 254, the Contractor must complete the SIPRNET Access Request Form, along with the modified DD Form 254, and forward to the KO prior to receiving access. A NATO awareness brief will also be required for all Contractors prior to access to the SIPRNET.

10. THIS CONTRACT WILL REQUIRE ACCESS TO:	**YES**	**NO**
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	☐	☐
b. RESTRICTED DATA	☐	☐
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	☐	☐
d. FORMERLY RESTRICTED DATA:	☐	☐
e. INTELLIGENCE INFORMATION:		
(1) Sensitive Compartmented Information (SCI)	☐	☐
(2) Non-SCI	☐	☐
f. SPECIAL ACCESS INFORMATION	☐	☐
g. NATO INFORMATION	☐	☐
h. FOREIGN GOVERNMENT INFORMATION	☐	☐
i. LIMITED DISSEMINATION INFORMATION	☐	☒
j. FOR OFFICIAL USE ONLY INFORMATION	☐	☐
k. OTHER (*Specify)*	☐	☐

Item 11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:

Mark all items “YES” or “NO” according to the contract requirements. (Coordinate with program and other security offices to ensure the appropriate controls are imposed on the contractor or subcontractor.) An explanation of each item follows.

11a. Have access to classified information only at another contractor’s facility or at a government activity. “ONLY” is the key word. Mark “YES” when access or storage of classified information is not required at the contractor’s facility. If marked “YES”:

(1) Item 1b should be marked “N/A” or “None.”

(2) When this item is marked YES, block 8a must identify the actual work location and if applicable block 8b and 8c must also be completed.

If 11a is “YES”, then 11b, 11c and, 11d, 11h and 11k will be “NO” – they are mutually exclusive. This question is about the safeguarding capability at the contractor facility. If no work is done at the contractor facility then they will not be receiving, generating, or fabricating anything classified at that location.

Enter the following statement in Item 13:

> **Ref 11a:** Contractor performance is restricted to (enter name and address of contractor facility or government activity). Government agency or activity will provide security classification guidance for performance of this contract. Submit visit request to the KO and/or Security Management Office for need-to-know verification.

11b. Receive classified documents only: "ONLY" is the keyword. Mark "YES" when the contractor will receive classified documents, (instead of classification guides), to perform on the contract, but is not expected to generate classified information. The classification markings shown on the documents received will provide the classification guidance necessary.

(1) If the volume or configuration of the documents is such that specialized storage requirements are necessary, contact DSS to verify storage capacity at the contracting facility.

(2) If this item is marked "YES", items 11a, 11c and 11d must be marked "NO".

If material is received and or stored at the contractor site for reference purposes only but the work is done on a government site or other cleared facility site, mark "YES". This item applies if there is no generation of classified materials (i.e. derivative classification).

Enter the following statement in Item 13:

> **Ref 11b:** Contractor will receive classified documents for reference only; however, if any classified information is generated in performance of this contract, it shall be derivatively classified and marked consistent with the source material.

11c. Receive and generate classified information**:** Mark "YES" when the contractor is expected to receive and generate classified material at the contractors' facility (documents and/or hardware) and will require detailed security classification guidance in order to perform on the contract. If this item is marked "YES," detailed security classification guidance must be provided. The guidance may be:

(1) Included in Item 13, and/or

(2) Attached to the DD Form 254, and/or

(3) Forwarded under separate cover, and/or

(4) Included in the contract document itself.

(5) If item 11c is marked “YES”, items 11a, 11b an 11e must be marked “NO”.

If the volume or configuration of the documents is such that specialized storage requirements are necessary, contact DSS to verify storage capacity at the contracting facility. Any applicable or additional guidance to the contractor should be included in Item 13

IMPORTANT: The contractor will be required to have safeguarding capability at its facility and the level of safeguarding required must be identified in item 1b.

Enter the following statement in Item 13:

Ref 11c: The contractor requires access to classified source data up to and including *(Top Secret, Secret, Confidential – insert one)* in support of the work effort. Any extracts or use of such data requires the contractor to apply derivative classifications and markings consistent with the source documents. Use of “Multiple Sources” on the “Derived From” line necessitates compliance with the NISPOM, paragraph 4-208a, and the use of a bibliography.

11d. Fabricate, modify, or store classified hardware: Mark “YES” if the contractor is expected to generate or utilize hardware which is classified due to its existence, uniqueness, appearance, application, capability, or product produced. Include as much information as possible (additional information can be added in Item 13) to describe the nature and extent of the storage that will be required.

(1) Will Restricted or Closed Areas be required?

(2) Is hardware involved and how much? How large is the hardware and can it be stored or will Open Storage be required?

(3) If item 11d is “YES”, items 11a, 11b and 11e must be marked “NO”.

If more than 2 cubic feet of storage is required, contact DSS to verify storage capacity at the contracting facility.

Enter the following statement in Item 13:

Ref 11d: Contractor must provide adequate storage at their facility for classified hardware to the level of (enter one: Top Secret, Secret, or Confidential).

11e. Perform services only: Mark “YES” if the contractor is performing a service only and is not expected to produce a deliverable item in accordance with the contract.

Enter a statement in Item 13 that explains the services provided and appropriate security guidance. Some examples are provided below:

Graphic Arts Services
"Reproduction services only. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract."

Engineering Services
"Contract is for engineering services. Classification markings on the material to be furnished will provide the classification guidance necessary for the performance of this contract."

Equipment Maintenance Services
"Contract is for equipment maintenance services on equipment which processes classified information. Actual knowledge of, generation, or production of classified information is not required for performance of the contract. Cleared personnel are required to perform this service because access to classified information can not be precluded by escorting personnel. Any classification guidance needed will be provided by the contractor."

Guard Services
"Contract is for guard services. Cleared personnel are required by the NISPOM to provide supplemental protection."

11f. Have access to U.S. classified information outside the U.S., Puerto Rico, U.S. Possessions and Trust Territories: If "YES," indicate in Item 13 the Army/U.S. activity, to include the city and country where the overseas performance will occur.

(1) If additional security requirements will be imposed on the contract, Item 14 must also be marked "YES" and completed as appropriate depending upon the programs involved.

(2) DSS does not provide oversight for contractors performing classified work outside of the U.S., Puerto Rico, U.S. Possessions and Trust Territories; therefore, any security reviews/inspections will have to be conducted by the supporting security office and Item 15 must be completed, designating the inspecting organization.

(3) For DoD contractors performing on overseas contracts, provide a copy of the DD Form 254 to the appropriate DSS Office of Industrial Security, International (See NISPOM Appendix A or contact DSS.)

(4) See NISPOM paragraph 10-204 for suggested "Security Clauses for International Contracts" for classified contracts involving foreign contractors.

11g. Be authorized to use the services of the Defense Technical Information Center (DTIC) or other secondary distribution center: Mark "YES" if the contractor is to be

authorized use of DTIC services. DD Form 1540 and DD Form 2345 must be completed for registration with DTIC.

(1) The sponsoring KO must submit DD Form 1540 “Registration for Scientific and Technical Information Services” to DTIC on behalf of the contractor. For subcontractors, the prime contractor submits the DD Form 1540 with the KO verifying the need-to-know.

(2) The contractor may also submit DD Form 2345 “Militarily Critical Technical Data Agreement” (after registration with DTIC) to the Defense Logistics Services Center for access to unclassified, militarily critical technical data from other DoD sources. The KO must certify the need-to-know to DTIC.

(3) See NISPOM Chapter 11, Section 2 for more information.

11h. Require a COMSEC account**:** Mark this item “YES” if the contractor is to be held accountable for COMSEC information. If non-accountable COMSEC information is involved, mark this item “NO.”

NOTE: Within the Army, COMSEC custodians are either DA civilians or military members. Contractors are considered hand receipt holders. See AR 380-40 for further guidance on COMSEC.

11i. Have TEMPEST Requirements: Mark “YES” if the contractor is required to impose TEMPEST countermeasures for information processing equipment after vulnerability assessments are completed. TEMPEST requirements are additional to the requirements of the NISPOM. The prime contractors may not impose TEMPEST requirements on their subcontractors without the KO approval.

(1) If marked “YES,” Item 14 must also be marked “YES” and pertinent contract clauses identified or added to Item 13.

(2) If requested by the KO, TEMPEST Countermeasure Assessment Requests may be included as an attachment to the DD Form 254.

TEMPEST - Electronic and electromechanical telecommunications and automated information processing equipment can produce unintentional, intelligence-bearing emanations, commonly known as TEMPEST. If intercepted and analyzed, these emanations may disclose information transmitted, received, handled or otherwise processed by the equipment.

Enter the following statement in Item 13:

> **Ref 11i:** TEMPEST Information is not releasable to contractor employees who have not received a FINAL Clearance at the appropriate security level. Written concurrence of the KO is required prior to subcontracting.

(1) 11j. Operations Security (OPSEC): Mark "YES" if the contractor must impose certain countermeasures directed to protect intelligence indicators. OPSEC requirements are additional to the requirements of the NISPOM. The prime contractors may not impose OPSEC requirements on their subcontractors unless the KO approves the OPSEC requirements. If marked "YES," Item 14 must also be marked "YES" and pertinent contract clauses identified or added to Item 13.

(2) If marked "YES", the pertinent OPSEC guidance must be listed in Item 13, if applicable.

Check if any special security guidance is required. It may require checking 10k as well. OPSEC requirements apply to National Industrial Security Program (NISP) contractors when it is determined that additional safeguards are essential for specific contracts; they are imposed in addition to the standard requirements of the NISP.

11k. Be authorized to use the Defense Courier Service (DCS): A "YES" in this block authorizes the contractor to use the services of DCS. The KO must obtain written approval from the Commander, Defense Courier Service, Attn: Operations Division, Fort George G. Meade, MD. 20755-5370. Only certain classified information qualifies for shipment by DCS. Prior approval of the KO is required before a prime contractor can authorize a subcontractor to use the services of DCS.

If the contractor is receiving materials through DCS then 1b should be marked "YES" to the appropriate safeguarding level (TS, S, or C). If this is marked "NO" then using DCS is not an option for the contractor.

11l. Other (Specify): Use this item to add any additional performance requirements not covered above. Annotate item 13 to provide any necessary remarks.

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	**YES**	**NO**
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	☐	☐
b. RECEIVE CLASSIFIED DOCUMENTS ONLY	☐	☐
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	☐	☐
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	☐	☐
e. PERFORM SERVICES ONLY	☐	☐

f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	☐	☐
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	☐	☐
h. REQUIRE A COMSEC ACCOUNT	☐	☐
i. HAVE A TEMPEST REQUIREMENT	☐	☐
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	☐	☐
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	☐	☐
l. OTHER *(Specify).*	☐	☐

Item 12. Public Release

The contractor is responsible for obtaining the approval of the KO prior to release of any information received or generated under the contract. The KO should complete this item as required by internal agency directives to direct the prime contractor to the appropriate office that has public release authority. Prime contractors should refer their subcontractors to the KO that was referenced in the prime contract DD Form 254.

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public release shall be submitted for approval prior to release
Through *(Specify):*
To the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* (Office of Freedom of Information; 1155 Defense Pentagon, Room 2C757; Washington, DC 20301-1155) for review. * In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

Item 13. Security Guidance

Use this block to expand or explain information marked "Yes" in blocks 10 and 11 of the DD Form 254. If the information does not fit into Block 13, annotate "See Attached Addendum" and provide all additional information accordingly. Be sure to: Identify the specific information to be classified; provide appropriate downgrading or declassification instructions; Security Classification Guidance; and provide any special instructions, explanations, comments, or statements necessary to clarify other items identified in the DD Form 254. **The information provided should be unclassified.** When completing Item 13 consider the following questions. In this case, more information is better. These questions should be asked when preparing guidance for a contractor:

(1) What classified information will the contractor need in the performance of this contract?

(2) Is there an existing Security Classification Guide for the Program?

(3) If subcontracting, is the guidance in the Prime Contract DD Form 254 adequate? Does the entire Prime Contract DD Form 254 apply to the subcontract or do you only need to provide applicable portions?

(4) Will classified source documents be used? If so, do they contain all the guidance the contractor needs?

(5) What will the contractor's actual performance be? (e.g., R&D, Test, Production, Study, etc.?)

(6) What unique characteristics are involved that need protection? Are there design features which require protection? Is there technical information which will require protection?

(7) What breakthroughs would be significant if achieved in an R&D effort?

(8) Are there performance limitations that require protection?

(9) Will classified hardware be furnished to or generated by the contractor?

(10) What information makes the hardware/services classified?

(11) Will hardware/data being generated require classification?

(12) At what stage in its production does hardware/data become classified?

Factors to consider when completing Item 13 include:

(1) Each contract is unique in its performance requirements. A standardized format may not necessarily be the best for every DD Form 254.

Give reasons for classification.

(1) Write guidance in plain easily understood English. Use additional pages to expand or explain guidance.

(2) Be specific as possible. Include only information pertaining to the contract.

(3) Avoid references to internal directives and instructions. If such documents provide guidance applicable to the contract, extract the pertinent portions and provide them as attachments. All documents cited in Item 13 should be provided to the contractor, either as attachments or forwarded under separate cover.

(4) Do not extract the requirements of the NISPOM or its supplements and include them in a DD Form 254. The NISPOM provides safeguarding requirements and procedures for classified information, not classification guidance.

(5) Encourage participation by the contractor in the preparation of the guidance and submission of comments and/or recommendations for changes in the guidance that has been provided.

Provide the points of contact information in Block 13 (Program Manager, COR/CM/COTR and those individuals who play a significant role in the contract). The COR/CM must sign in block 13 acknowledging they have reviewed the DD Form 254 and are in agreement and provide the following statement: "The undersigned has reviewed this Security Specification, understands the provisions and will ensure that it is complied with within the limits of his/her responsibility, and that any violations are brought to the attention of the KO and supporting Security Manager."

Use this section to explain anything that might be unclear, confusing, or particularly important. Be careful not to include anything that could be interpreted as a contradiction to information elsewhere on this form. This section can extend to additional pages if needed. There is no set page limit.

Provide any training requirements for contractors relating to the mission and/or contractual duties (i.e., COMSEC hand receipt holders, Information Assurance, AT/FP, etc.).

The DD Form 254 is a legal document and part of the contract. It is the source of security requirements and guidance that the contractor receives from the Army. Include names of pertinent manuals, page numbers, and other helpful designations (be sure to attach all referenced materials).

If additional space is required for Item 13, note the attachment(s) at the end of Item 13. The contract number must be placed at the top of each Attachment page to ensure proper identification if inadvertently separated from the DD Form 254. Number the pages as needed.

Example of Attachment Page Header: CONTINUATION OF BLOCK 13 OF THE DD FORM 254 Solicitation or Contract #

When providing additional guidance in Item 13 or the Attachment, identify the item number being expanded upon. (i.e., Item 10j: FOUO…)

List the Security Classification Guides (SCGs) applicable to the performance of the contract.

Additional "Actual Performance Locations" (items 8a, 8b and 8c) should be listed in Item 13. For SCI contracts, list all performance locations in item 11 of the SCI Addendum.

If there are additional "required distributions" (Item 17f), list in item 13 or add an Attachment page.

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

Item 14. Additional Security Requirements

Complete this item when security requirements are imposed on a contractor in addition to the requirements of the NISPOM or its supplements.

Additional requirements translate into additional costs. It is essential for coordination with the program and other security offices to ensure the appropriate security requirements are imposed on the contractor.

(1) A "YES" in this item requires the KO or prime contractor to incorporate the additional requirements in the contract itself or to incorporate the additional requirements by statements or reference in Item 13.

(2) Costs incurred due to additional security requirements are subject to negotiation between the contractor and the KO.

(3) Prior approval of the KO is required before a prime contractor can impose additional security requirements on a subcontractor.

(4) A copy of the DD Form 254 containing the additional security requirements will be provided to the KO.

SAP or SCI are examples of programs and information that would require additional security requirements.

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

Item 15. Inspections

Mark "YES" if DSS is relieved, in whole or in part, of the responsibility to conduct security reviews and provide security oversight to the contractor. Information should be provided regarding the specific areas from which DSS is excluded and the agency that will assume the responsibility.

DSS is relieved of the responsibility to inspect:

(1) SCI material. When access to SCI is required (Item 10e (l)), **the following statement must be added:** "(Enter appropriate Agency/Military Department Senior Intelligence Officer) has exclusive security responsibility for SCI classified material released or developed under this contract and held within the contractor's SCIF." DSS will inspect SCI if there is an agreement with the program office and CSE. (2) Special Access Programs where DSS is "carved out" from inspection responsibility. Not all Army SAPs are "carve outs". In some instances, the cognizant SAP security office will allow DSS to retain inspection responsibility. If Block 15 is checked "YES" the KO must provide the approval and reporting of the "carve-out".

(3) Contractor facilities operating on military installations when the installation Commander has elected to retain security cognizance. It is the responsibility of the supporting ISS to maintain copies of all inspections performed on the program during the life of the DD Form 254. The ISS will ensure the KO receives copies of the inspection reports.

In all cases, provide DSS a copy of the DD Form 254.

If inspections will be conducted by an organization other than DSS, complete Item 15. An inspection by an agency other than DSS does not change DSS' designation as CSO and does not relieve the KO from the responsibility of providing a copy of the DD Form 254 to DSS.

When an Army Commander has determined to retain oversight and inspection of a cleared contractor facility, the supporting ISS, who is responsible for the inspections and oversight of the cleared facility, will brief key DA, KO and the PM/PEO on the status of the cleared contractor security program. The ISS will retain copies of the inspections and provide a copy of reviews and other related assessments to the KO. A copy of the inspection report is normally not provided to DSS unless extenuating circumstances exist.

The POC, supporting security office and the organization responsible for inspections must be listed in block 15. Use block 13 on an Attachment page if additional space is needed.

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

Item 16. Certification and Signature

Enter the name, title, telephone number, address and signature of the Security Manager. The Security Manager is the official certifying that the security requirements are complete and adequate for performance of the classified contract. The Army Federal Acquisition Regulation Supplement (AFARS) designates the Security Manager sign in block 16.

The KO must ensure that the DD Form 254 has been adequately staffed among the appropriate contracting, program and security personnel.

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 Date Signed:	b. TITLE IAW AFAR , Paragraph 5104.403 (*22 May 2007*)	c. TELEPHONE *(Include Area Code)*
d. ADDRESS *(Include ZIP Code)*		

DD Form 254 (BACK), DEC 1999

Item 17. Required Distribution

The KO will distribute copies of the DD Form 254, as appropriate, indicating the distribution in the respective blocks. Additional copies can be distributed internally to the visit control office, contracts department, department heads, etc. If this is a SAP contract, TMO must be annotated as a required distribution. Ensure a copy of the DD Form 254 is provided to the government supporting security office for all designated performance locations listed in Item 8.

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 KOR
- ☐ f. OTHERS AS NECESSARY

CHAPTER 5

ACRONYMS: Security related acronyms, abbreviations and basic terms used in this guide.

ACA – Army Contracting Activity
AFARS – Army Federal Acquisition Regulation Supplement
AR – Army Regulation
CAGE - Commercial and Government Entity
CM - Contract Monitor
CNWDI - Critical Nuclear Weapon Design Information
COMSEC - Communications Security
COR - Contracting Officer Representative
CSA - Cognizant Security Agency
CSO - Cognizant Security Office
CVA - Central Verification Activity
DCI - Director of Central Intelligence
DCS - Defense Courier Service
DD - Defense Department
DFARS – Defense Federal Acquisition Regulation Supplement
DNI – Director of National Intelligence
DSS - Defense Security Service
DTIC - Defense Technical Information Center
FAR – Federal Acquisition Regulation
FOUO - For Official Use Only
FRD - Formerly Restricted Data
GCA - Government Contracting Agency
IFB - Invitation for Bid
IR&D - Independent Research and Development
ISS - Industrial Security Specialist
KO - Contracting Office, or the designee
LIMDIS - Limited Distribution
NATO - North Atlantic Treaty Organization

NISPOM - National Industrial Security Program Operating Manual

OISI - Office of Industrial Security International

OPSEC - Operations Security

PSO - Program Security Officer

RD - Restricted Data

RFP - Request for Proposal

RFQ - Request for Quote

SAP - Special Access Program

SCI - Sensitive Compartmented Information

TCAR - TEMPEST Countermeasure Assessment Request

TMO – Technology Management Office

CHAPTER 6

Definitions:

Classified Contract - Any contract, subcontract, purchase order, lease agreement, service agreement, etc., that requires or will require access to classified information by a contractor or his or her employees in the performance of the contract. (A contract may be classified even though the contract document is not classified). This term is used throughout the NISPOM because it is the most common situation where a contractor has access to or possession of classified information. However, the requirements prescribed for a "classified contract" also are applicable to all phases of pre-contract activity, including solicitations (bids, quotations, and proposals), pre-contract negotiations, post-contract activity, or other Government Agency program or project which requires access to classified information by the contractor.

Classified Information - Any information that is owned by, produced by or for, or under the control of the U.S. Government, and determined pursuant to Executive Order 12958, or prior orders, to require protection against unauthorized disclosure, and is designated as TOP SECRET, SECRET or CONFIDENTIAL.

Cleared Contractor - Any corporation, company, contractor, consultant, individual or their employees, agents, representatives (actual or potential) who require or will require access to classified information in the performance of a contract.

CNWDI - Critical Nuclear Weapon Design Information. A DoD category of weapon data designating TOP SECRET Restricted Data or SECRET Restricted Data revealing the theory of operation or design of the components of a thermonuclear or implosion-type fission bomb, warhead, demolition munitions, or test device.

COMSEC - Communications Security. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government relating to national security and to ensure the authenticity of such communications.

Contract Monitor- Appropriately indoctrinated personnel (military or civilian) appointed by the KO to monitor the day-to-day activities of all assigned contracts including those at the SCI and SAP level. A COR/CM may be the same person dependent upon command requirements. Serve as a POC for Contractor Special Security Officer/Facility Security Officer/Security Point Of Contact.

Cognizant Security Agency - Agencies of the Executive Branch that have been authorized to establish and industrial security program to safeguard classified information under the jurisdiction of those agencies when disclosed or released to U.S. industry. These agencies are: The Department of Defense, Department of Energy, Central Intelligence Agency and the Nuclear Regulatory Commission.

Cognizant Security Office – The office or offices delegated by the Head of a Cognizant Security Agency to administer industrial security on behalf of the Cognizant Security Agency.

Contracting Officer – A government official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts and make determinations and findings with respect thereto, or any part of such authority. Who has a valid appointment as a Contracting Officer under the provisions of the Federal Acquisition Regulation. The individual has the authority to enter into and administer contracts and determinations as well as findings about such contracts.

Contracting Officer Representative - An individual who is designated and authorized in writing by the Contracting Officer to perform specific technical or administrative functions on contracts or orders.

Contractor – Any industrial, educational, commercial, or other entity that has been granted a facility clearance (FCL) by a CSA.

Facility Security Clearance (FCL) - An administrative determination that, from a security viewpoint, a facility is eligible for access to classified information of a certain category and all lower categories.

Final DD FORM 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to provide classification guidance and security requirements to contractors who wish to retain classified information beyond the terms of the contract as authorized by the NISPO

Foreign Government Information - Information that is:

a. Provided to the U.S. by a foreign government or governments, an international organization or government, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

b. Produced by the U.S pursuant to, or as a result of, a joint arrangement with a 20governments or any element thereof requiring that the information, the arrangement, or both are to be held in confidence.

Formerly Restricted Data - Classified information jointly determined by the DoE and its predecessors and the DoD to be related primarily to the military utilization of atomic weapons and removed by the DOE from the Restricted Data category pursuant to section 142(d) of the Atomic Energy Act of 1954, as amended, and safeguarded as National Security Information, subject to the restrictions on transmission to other countries and regional defense organizations that apply to Restricted Data.

For Official Use Only - Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from public disclosure under the criteria of the Freedom of Information Act, Title 5, U.S.C., Section 552.

Government Contracting Agency (GCA) – Activity responsible for awarding a contract.

Industrial Security - That portion of internal security that is concerned with the protection of classified information in the hands of U.S. industry.

Industrial Security Specialist - Responsible for implementing the installation or unit Industrial Security Program and for managing and providing oversight of contractors performing classified contractual activities on Army installations or within activities, to ensure compliance with governing security regulations.

NATO Classified Information - The term “NATO classified information” embraces all classified information, military, political and economic that is circulated within an by NATO whether such information originates in the organization itself or is received from member nations or from other international organizations.

NATO Information - Information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless proper NATO authority has been obtained to release outside of NATO.

OPSEC - Operations Security - A security discipline designed to identify and analyze intelligence indicators which may have a bearing on the security integrity of a classified program. The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling and protecting indicators associated with planning and conducting military operations and other activities.

Original DD FORM 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to provide original classification guidance and security requirements on a classified contract. Original DD FORM 254s are issued during the solicitation phase of a contract to provide classification guidance and security requirements to prospective contractors as they formulate their bids. Once the contract is awarded, another Original DD FORM 254 is issued to the contractor who is being awarded the contract.

Prime Contract - A contract let by a KO to a contractor for a legitimate government purpose.

Prime Contractor - Any contractor who has received a prime contract from a Government Agency. For purposes of subcontracting, a subcontractor shall be considered to be a prime contractor in relation to its subcontractor.

Restricted Data - All data concerning the design, manufacture, or utilization of atomic weapons; the production of special nuclear material; or the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the RD category pursuant to section 142 of the Atomic Energy Act of 1954, as amended.

Revised DD FORM 254 - A Contract Security Classification Specification that is issued by a Government Contracting Activity or a Prime Contractor to change classification guidance and security requirements on a classified contract.

SAP - Special Access Program - Any program that is established to control access, distribution, and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET OR CONFIDENTIAL information. A special Access Program can be created or continued only as authorized by the Deputy Secretary of Defense pursuant to E.0. 13526.

SCI - Sensitive Compartmented Information – Classified national intelligence concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence (The Intelligence Community Standard 2008-700-1, dated 8/4/2008).

Subcontract - A contract entered into by a contractor to furnish supplies or services for performance of a prime contract or other subcontract

Subcontractor – A supplier, distributor, vendor or firm that furnishes supplies or services to or for a prime contractor.

TEMPEST - An unclassified short name referring to investigations and studies of compromising emanations. Compromising emanations are unintentional intelligence-bearing signals that, if intercepted and analyzed, will disclose classified information when it is transmitted, received, handled, or otherwise processed by any information processing equipment.

CHAPTER 7

Additional Information

Verification of primary contractor additional performance locations: The ISS who processes the DD Form 254 will verify through ISFD that the companies citied on the DD Form 254 possess the appropriate clearances prior to signing the DD Form 254.

CAGE CODE: All cage codes are five (5) digits long and begin and end with a number.

Blanket Purchase Agreement (BPA) and General Services Administration (GSA) contracts are “open-end” or Call –Type contracts. A single DD Form 254 may be used to cover a Basic Ordering Agreement (BOA) or an indefinite delivery contract, except when the individual call, purchase order, or request for services or products requires classification specification different from that provided for the overall contract. A DD Form 254 will not be issued for unclassified task orders, delivery orders, etc.

Additional Performance Locations: Some contractor facilities have off-site locations that handle and store classified information but do not possess a unique cage code. These off site locations fall under the security umbrella of the prime contractor and must be within a 60-minute drive from the primary facility. The primary Facility Security Officer (FSO) has security over site of these locations. The User Agency will communicate with the primary facility only. The off-site location will not be cited on the DD Form 254.

Access to COMSEC, CNWDI and NATO information requires a briefing prior to receiving any information.

Accountable COMSEC information: Keying material, CCI (Controlled Cryptographic Item) Material and CRYPTO.

- If the COMSEC material is accountable but the contractor only has access to it at the User Agency, then item 10a is marked “YES” and 11h is marked “NO”.
- If the COMSEC material is accountable and the contractor has access to it at the contracting facility, then item 10a is marked “YES” and item 11h is marked “YES”.

NOTE: Contractors are hand receipt holders and not COMSEC Custodians. See AR 380-40 for further clarification.

Secure telephones (STEs):

- If the contractor will be using secure telephone equipment at the contractor facility, but the equipment is owned by the User Agency, then item 10a is marked “YES” and item 11h is marked “NO”.
- If the contractor will be using secure telephone equipment at the contractor facility and the equipment is owned by the contractor, then item 10a is marked “YES” and item 11h is marked “YES”.

Additional Information for block 13 (to be used as appropriate):

- Contract performance is restricted to: (list where restriction(s) are/is)
- User agency will provide security classification guidance for performance of this contract
- All classified material/information shall be provided by the user agency and shall be safeguarded at the user agency.
- Any classified information generated in performance of this contract shall be classified in accordance to the markings shown on the source material.
- Foreign visits will be conducted in accordance with the U.S. Army Foreign Disclosure Regulation, AR 380-10.

APPENDIX A
EXAMPLE OF US ARMY SAP ADDENDUM TO DD FORM 254

XXX (1) This contract requires access to Special Access Program information (SAPI). The Commander, US Army Training and Doctrine Command (TRADOC)(Fill in the name of the contracting command or activity), as the Cognizant Security Authority (CSA) for the US Army for this contract, has security oversight and management responsibility for all SAPI released to the contractor or developed under this contract, held within the Contractor's SAP Facility (SAPF) or in SCIF or SAPF under a Co-utilization Agreement (CUA). TRADOC is acting on behalf of the Technology Management Office (TMO), the Army Special Access Program Coordination Office (SAPCO) which is responsible for security oversight and management for Army SAPs. Under this contract, the Defense Security Service (DSS) is responsible for security compliance inspections of contractor SAP facilities. DSS retains responsibility for all collateral information released or developed under the contract. The contracting organization will assist the government when conducting threat and vulnerability surveys. The manuals, regulations and directives checked below provide the necessary guidance for physical, personnel, and information security for safeguarding SAPI, and are part of the security classification specification for this contract:

XXX DoD 5220.22-M-1, NISPOM, with DoD overprint and NISPOMSUB
XXX JAFAN 6/3, Protecting Special Access Program Information within Information Systems
XXX JAFAN 6/4, Special Access Program Tier Review Process
XXX JAFAN 6/9, Physical Security Standards for Special Access Program Facilities, w/ change 2
XXX AR 25-2, Information Assurance
XXX AR 380-28, DA Special Security System
XXX AR 380-381, Special Access Programs (SAPS) and Sensitive Activities.
XXX Other

XXX (2) Contract estimated completion date: TBD by prime contract

XXX (3) The name, telephone number, email address and mailing address of the Contract Monitor (CM) for the SAP portion of this contract is: John Smith, Program Security Manager (PSM), 757-555-5555. NIPR: John.Smith@mi.army.mil / SIPR: john.smith@mi.army.smil.mil. (The Contract Monitor and the contractor security officer must be registered in the Army Contractor Automated Verification System (ACAVS) in order to process SAP actions)

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SAP under this contract must be forwarded to the PSM for approval and then to the Contracting Officer and Program Manager for review and concurrence prior to award of the subcontract.

XXX (5) The contractor will submit the request for SAP visit certifications through the PSM for approval of the visit. The certification request must arrive at the PSM at least ten (10) working days prior to the visit. Visit certification requests will be processed through ACAVS.
XXX (6) The contractor will not reproduce any SAPI related material without prior written permission of the CM.
XXX (7) Security Classification Guides or extracts are attached or will be provided under separate cover.
XXX (8) Electronic processing of SAP requires accreditation of the equipment in accordance with JAFAN 6/3 and AR 25-2. (Note: Check only if item 11l indicates that a requirement exists for SAP AIS processing.)
XXX (9) This contract requires a contractor SAPF.
XXX (10) This contract requires indoctrination to ZGD(U) Special Access Program.
XXX (11) The contractor will perform SAPI work under this contract at the following locations: (list all locations)

APPENDIX B
INSTRUCTIONS FOR THE US ARMY SCI ADDENDUM TO DD FORM 254

General: This section contains specific instructions for preparation of the “SCI Addendum," used in conjunction with the DD Form 254, for all Army SCI contracts and their related SCI subcontracts.

a. The SCI addendum is designed for use with the DD Form 254 on all Army SCI contractual efforts and their related subcontracts. The User Agency and the appointed CM are responsible for coordinating with HQ INSCOM, ACofS Security, G2, Contractor Support Element (CSE) for developing and incorporating the SCI addendum with an appropriate DD Form 254 for the prime contract.

b. Based on the guidance provided in the DD Form 254 and SCI addendum for the prime contract, the contractor (prime) is responsible for coordinating with the CM and the CSE for developing and incorporating the SCI addendum with an appropriate DD Form 254 for all related subcontracts.

This document must be executed and accompany all DD Forms 254 issued for Request for BID (RFB), Request for Proposal (RFP), Request for Quotation (RFQ), etc., and forwarded with the DD Form 254 to the CSE prior to award of an Army SCI contract. Those items that are pre “X’d”, apply to all Army SCI contracts/subcontracts.

Item 1: Regulations listed that are not marked, are to be marked with an “X “when they apply.

Imagery Policy Series (Available from the CM): Applies when the contract/subcontract requires TK level SCI (i.e. access, documents etc.)

DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities. Required when the contractor is authorized a Sensitive Compartmented Information Facility (SCIF).

DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems, applies when AIS processing is involved.

DIAM 50-4, Security of Compartmented Computer Operations: Applies when the contract/subcontract requires the contractor to process SCI electronically utilizing computer equipment within an accredited SCIF. (See item 11l of the DD Form 254.)

DIAM 50-24, Security for Using Communication Equipment in a SCIF: Applies when and if a contractor/subcontractor intends the use of a modem connected to an unencrypted black telephone line and/or the use of secure telephone unit data port within an accredited SCIF.

AR 25-2, Information Assurance: Applies when item 11l of the DD Form 254 is marked “Yes”.

AR 380-381, Special Access Programs (SAPS): Applies when item 10f of the DD Form 254 is marked “Yes”.

Item 2: An estimated completion date must be annotated. Do not include proposed option years. An option is not official until it is exercised by the government.

Item 3: The name, official organization address, email address and telephone number of the designated Contract Monitor (CM) by the User Agency (contracting agency/ office). NOTE: The CM designated must be either military or a DA civilian, who possess the appropriate SCI access to the levels required by the contract. Further, the CM for the prime contract is always the CM for all related subcontracts. Additionally, in this item, identify the Security POC, with telephone number and email address, at the company to be awarded the contract/subcontract.

Item 4: When a subcontract for a portion of the SCI contract is to be authorized, prior to award of the subcontract, the prime contractor must execute and forward a DD Form 254 for the proposed subcontract through the prime contract CM, for his/her approval, to the CSE for concurrence.

Item 5: Cites requirement for SCI visit certifications.

Item 6: Identifies the requirement for prior written authority to reproduce SCI and all related material.

Item 7: Identifies whether or not classification guide(s) or extract(s) exist for this specific contract and how they are to be obtained by the contractor.

Item 8: Cites the requirement to have an accreditation of all electronic processing equipment prior to the processing SCI by the contractor.

Item 9: Identifies the requirement for the contractor to have their own accredited SCIF or co-utilized SCIF to execute the SCI portion of the contract.

Item 10: Cites the accesses required for execution of the contract, mark what accesses are required for performance on the contract/subcontract. Further, allows the *option* of citing an estimated number of accesses required

Item 11: Requires identification, in addition to Item 8 of the DD Form 254, of any additional locations where SCI work for this specific contract will be conducted.

CONTRACT # TBD
SOLICITATION #

EXAMPLE OF US ARMY SCI ADDENDUM TO DD FORM 254, (date)

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

XXX DoD 5105.21-M-1, SCI Security Manual, Administrative Security
XXX Signals Intelligence Security Regulations (SISR) (Available from the CM)
XXX Imagery Policy Series (Available from the CM)
XXX DCID 6/3, Protecting Sensitive Compartmented Information within Information Systems
XXX DCID 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities
XXX AR 25-2, Information Assurance
XXX AR 380-28, DA Special Security System
XXX AR 380-381, Special Access Programs (SAPS).
XXX Army Handbook for SCI Contracts.
XXX Other

XXX (2) Contract estimated completion date: **TBD** (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:

CM: LIST NAME, PHONE NUMBER, TITLE, OFFICE SYMBOL, ADDRESS, CITY/STATE/ZIP CODE, EMAIL ADDRESS

SCTY POC: TBD (Identify the Security POC & phone number and email address at the contractor’s/subcontractor’s location)

(The Contract Monitor and the contractor security officer must be registered in the Army Contractor Automated Verification System (ACAVS) in order to process SCI actions)

XXX (4) All DD Forms 254 prepared for subcontracts involving access to SCI under this contract must be forwarded to the CM for approval and then to HQ INSCOM, ACofS Security, G2, 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. Visit certification requests will be processed through ACAVS.

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

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

XXX (8) Electronic processing of SCI requires accreditation of the equipment in accordance with DCID 6/3 and AR 25-2 (Note: Check only if item 11l indicates that a requirement exists for SCI IS processing.)

XXX (9) This contract requires a contractor SCIF.

XXX (10) This contract requires **XX** (SI) ___ (TK) ___ (G) ___ (HCS) (Add others as required)

XXX (11) The contractor will perform SCI work under this contract at the following locations: TBD (Identify the location and CAGE code)