

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING a. FACILITY CLEARANCE REQUIRED b. LEVEL OF SAFEGUARDING REQUIRED		
2. THIS SPECIFICATION IS FOR: <i>(X and complete as applicable)</i>				3. THIS SPECIFICATION IS: <i>(X and complete as applicable)</i>		
a. PRIME CONTRACT NUMBER				a. ORIGINAL <i>(Complete date in all cases)</i>	DATE (YYYYMMDD)	
b. SUBCONTRACT NUMBER				b. REVISED <i>(Supersedes all previous specs)</i>	REVISION NO. DATE (YYYYMMDD)	
c. SOLICITATION OR OTHER NUMBER		DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 5 in all cases)</i>	DATE (YYYYMMDD)	
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received or generated under _____ <i>(Preceding Contract Number)</i> is transferred to this follow-on contract.						
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____						
6. CONTRACTOR <i>(Include Commercial and Government Entity (CAGE) Code)</i>						
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
7. SUBCONTRACTOR						
a. NAME, ADDRESS, AND ZIP CODE			b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
8. ACTUAL PERFORMANCE						
a. LOCATION			b. CAGE CODE	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT						
10. CONTRACTOR WILL REQUIRE ACCESS TO:			YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION					a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	
b. RESTRICTED DATA					b. RECEIVE CLASSIFIED DOCUMENTS ONLY	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION					c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	
d. FORMERLY RESTRICTED DATA					d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	
e. INTELLIGENCE INFORMATION					e. PERFORM SERVICES ONLY	
(1) Sensitive Compartmented Information (SCI)					f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	
(2) Non-SCI					g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	
f. SPECIAL ACCESS INFORMATION					h. REQUIRE A COMSEC ACCOUNT	
g. NATO INFORMATION					i. HAVE TEMPEST REQUIREMENTS	
h. FOREIGN GOVERNMENT INFORMATION					j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	
i. LIMITED DISSEMINATION INFORMATION					k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	
j. FOR OFFICIAL USE ONLY INFORMATION					l. OTHER <i>(Specify)</i>	
k. OTHER <i>(Specify)</i>						

12. PUBLIC RELEASE. Any information (*classified or unclassified*) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release Direct Through (*Specify*)

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

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

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

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

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

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (<i>Include Area Code</i>)
d. ADDRESS (<i>Include Zip Code</i>)	17. REQUIRED DISTRIBUTION <input type="checkbox"/> a. CONTRACTOR <input type="checkbox"/> b. SUBCONTRACTOR <input type="checkbox"/> c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR <input type="checkbox"/> d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION <input type="checkbox"/> e. ADMINISTRATIVE CONTRACTING OFFICER <input type="checkbox"/> f. OTHERS AS NECESSARY	
e. SIGNATURE		

Continuation: Draft SNIM IDIQ Master DD 254
Contract: TBD

Cognizant COTR/Program Manager: TBD

Defense Technical Information Center
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218
Phone (703) 767-9200

Ref 13 (cont): All transportation or transmission of classified information/material to and from government/contractor facilities shall be conducted IAW NISPOM. DTIC Contracting Activity will be notified prior to any portion of this contract being subcontracted out.

Ref 10a: COMSEC security requirements apply. Contractor must forward requests for COMSEC material/information to the appropriate COMSEC officer through the program office. The contractor is governed by DoD 5220.22-M, NISPOM. Access to COMSEC material by personnel is restricted to U.S. citizens holding final U.S. Government clearances. Such information is not releasable to personnel holding only reciprocal clearances. The government program/project manager shall designate the number of personnel requiring cryptographic access. The number will be limited to the minimum necessary and will be on a strict need-to-know basis. Additional COMSEC requirements may be required at some locations/facilities (based on service/command requirements). The Performance Monitor or component command COR at these locations/facilities will provide specific information.

Ref 10e(1) & (2): Left intentionally blank. Individual Tasks will guide requirements dependent upon access requirements. At a minimum, Contractor will require DCID 6/6. Prior approval of the contracting activity is required for sub-contracting. Access to intelligence information requires special briefings and a final US Government clearance at the appropriate level. If block 10e(2) is checked, then a separate SCI Addendum will be issued to the Contractor.

Ref 10j: FOUO information/provided under this contract shall be safeguard as specified in Attachment 2, Protecting For Official Use Only (FOUO) Information.

Ref 11c: Left intentionally blank. The individual Task will determine requirements.

Ref 11g: Left intentionally blank. If necessary, the contractor will need to submit a DD Form 1540, *Registration for Scientific and Technical Information Services* to the Defense Technical Information Center in accordance with the NISPOM.

Continuation: Draft SNIM IDIQ Master DD 254
Contract: TBD

Ref 11h: Left intentionally blank. If accountable COMSEC material will be provided to the contractor, mark “YES” in **Item 11h**. If accountable COMSEC is involved, the contractor must establish a COMSEC account. An X in the YES box imposes the requirements of **DoD 5220.22-M, NISPOM**. Further disclosure, to include subcontracting of COMSEC material for a contractor, requires prior approval of the contracting activity. Access to COMSEC material requires special briefings. Access to classified COMSEC material requires a final U.S. Government clearance at the appropriate level

Ref 11j: Certain aspects concerning the customer will be unclassified; however, compilation of information as well as links between the customer and various components of the program are sensitive and require protection as FOUO information.

Ref 11k: Left intentionally blank. Item 11k will be marked “YES” only when items 1a and 1b are marked **Top Secret** and/or when both **Items 10a and 11h (COMSEC)** are marked “YES.” Only certain classified information qualifies for shipment by DCS. It is the responsibility of the contracting activity to comply with DCS policy and procedures. This item authorizes the contractor to use the services of DCS. “YES” in this item requires the contracting activity to request DCS services from:

Commander, Defense Courier Service
Attn: Operations Division
Fort George G. Meade, MD 20755-5370

Ref 14: While performing at Military Service owned and/or operated locations/facilities, the contractor will adhere to the respective Military Service: Information Security Program, ADP Programs, Physical Security Program, and Industrial Security Program. Appropriate local service/component command security directives, regulations, and standard operating procedures will be provided by the requiring agency (as needed) at these locations/facilities. Prior approval of the contracting activity is required for subcontracting. Access to intelligence information requires special briefings and a U.S. Government clearance at the appropriate level.

-- LAST ITEM --

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 it must be reviewed by the Government prior to its release to determine whether a significant and legitimate government purpose is served by withholding the information or portions of it.

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). No portion markings will be shown.
- 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."

Continuation: Draft SNIM IDIQ Master DD 254
Contract: TBD

- 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.

Continuation: Draft SNIM IDIQ Master DD 254
Contract: TBD

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.

-- LAST ITEM --