

|   |  |
|---|--|
| <p><b>DEPARTMENT OF DEFENSE</b></p> <p><b>CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b></p> <p><i>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</i></p> | <p><b>1. CLEARANCE AND SAFEGUARDING</b></p> <p>a. FACILITY CLEARANCE REQUIRED<br/>SECRET</p> <p>b. LEVEL OF SAFEGUARDING REQUIRED<br/>SECRET</p> |
|---|--|

|  |   |
|--|---|
| <b>2. THIS SPECIFICATION IS FOR:</b> (X and complete as applicable)            | <b>3. THIS SPECIFICATION IS:</b> (X and complete as applicable)       |
| a. PRIME CONTRACT NUMBER   | X a. ORIGINAL (Complete date in all cases) Date (YYMMDD)<br>030515    |
| b. SUBCONTRACT NUMBER  | b. REVISED (Supersedes all previous specs) Revision No. Date (YYMMDD) |
| X c. SOLICITATION OR OTHER NUMBER<br><b>M67854-03-R-7041</b> Due Date (YYMMDD) | c. FINAL (Complete item 5 in all cases) Date (YYMMDD)                 |

**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.

**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 \_\_\_\_\_.

**6. CONTRACTOR** (Include Commercial and Government Entity (CAGE) Code)

|  |              |  |
|--|--------------|--|
| a. NAME, ADDRESS, AND ZIP CODE<br><b>TBD</b> | B. CAGE CODE | C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) |
|--|--------------|--|

**7. SUBCONTRACTOR**

|                                |              |  |
|--------------------------------|--------------|--|
| a. NAME, ADDRESS, AND ZIP CODE | B. CAGE CODE | C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) |
|--------------------------------|--------------|--|

**8. ACTUAL PERFORMANCE**

|                                |              |  |
|--------------------------------|--------------|--|
| a. NAME, ADDRESS, AND ZIP CODE | B. CAGE CODE | C. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) |
|--------------------------------|--------------|--|

**9. GENERAL IDENTIFICATION OF THE PROCUREMENT** Production of the Transition Switch Module (TSM). The scope of work includes support of the Government conducted Joint Interoperability Certification, Operational Test & Evaluation (OT&E) and retrofit of the Engineering Development Models (EDMs) to the final configuration of the TSM following OT&E and environmental testing.

| 10. THIS CONTRACT WILL REQUIRE ACCESS TO:            | YES | NO | 11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:  | YES | NO |
|--|-----|----|--|-----|----|
| a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION      | X   |    | a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY                    |     | X  |
| b. RESTRICTED DATA                                   |     | X  | b. RECEIVE CLASSIFIED DOCUMENTS ONLY   |     | X  |
| c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION        |     | X  | c. RECEIVE AND GENERATE CLASSIFIED MATERIAL  | X   |    |
| d. FORMERLY RESTRICTED DATA                          |     | X  | d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE   | X   |    |
| e. INTELLIGENCE INFORMATION:                         |     |    | e. PERFORM SERVICES ONLY   |     | X  |
| (1) Sensitive Compartmented Information (SCI)        |     | X  | f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES        | X   |    |
| (2) Non-SCI  |     | X  | g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER | X   |    |
| f. SPECIAL ACCESS INFORMATION                        |     | X  | h. REQUIRE A COMSEC ACCOUNT  | X   |    |
| g. NATO INFORMATION                                  |     | X  | i. HAVE TEMPEST REQUIREMENTS   |     | X  |
| h. FOREIGN GOVERNMENT INFORMATION                    |     | X  | j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS   |     | X  |
| i. LIMITED DISSEMINATION INFORMATION                 |     | X  | k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE  |     | X  |
| j. FOR OFFICIAL USE ONLY INFORMATION                 | X   |    | l. OTHER (Specify)   | X   |    |
| k. OTHER (Specify) AIS Requirements – Attachment "B" | X   |    | See Item # 13.   |     |    |

**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):

Commanding General, MARCORSYSCOM (LAW-Q)  
 2033 Barnett Ave Suite 315  
 Quantico VA 22134-5010

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.)

See attached continuation Sheet.

**14. ADDITIONAL SECURITY REQUIREMENTS.** Requirements identify the pertinent contracted 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

**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

**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<br>SUSAN JONES | b. TITLE<br>Security Specialist | c. TELEPHONE (Include Area Code)<br>(703) 432-4161 |
|---|---------------------------------|--|

d. ADDRESS (Include Zip Code)  
 MARCORSYSCOM (00U)  
 2033 Barnett Ave Suite 315  
 Quantico VA 22134-5010

e. SIGNATURE  


**17. REQUIRED DISTRIBUTION**

|                                     |   |
|-------------------------------------|---|
| <input checked="" type="checkbox"/> | a. CONTRACTOR   |
| <input type="checkbox"/>            | b. SUBCONTRACTOR  |
| <input checked="" type="checkbox"/> | c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR          |
| <input type="checkbox"/>            | d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION |
| <input checked="" type="checkbox"/> | e. ADMINISTRATIVE CONTRACTING OFFICER                             |
| <input checked="" type="checkbox"/> | f. OTHERS AS NECESSARY  |

**CONTINUATION SHEETS FOR  
CONTRACT M67854-03-R-7041**

Security classification guides required during this contract will be provide under separate cover by the project officer.

In addition to the reporting requirements directed by the NISPOM, the contractor will provide a concurrent report of loss or compromise of classified information to the Commanding General, Marine Corps Systems Command (Attn: Security Manager), 2033 Barnett Ave Suite 315, Quantico VA 22134-5010.

Visit requests to activities other than MARCORSYSCOM shall have "Need to Know" certified by Commanding General, MARCORSYSCOM (SECURITY). All requests shall contain the information required by the NISPOM and shall not exceed a 12 month period.

All Government Badges issued under this contract will be returned immediately to the MARCORSYSCOM CENTRAL SECURITY STATION upon termination of contract, or individual terminations. When an individual contractor is terminated, for any reason, it is the responsibility of the Facility Security Officer to immediately notify the Command Security Manager, MARCORSYSCOM 2033 Barnett Ave Suite 315, Quantico VA 22134-5010. Failure to comply could result in the suspension of all contractor proximity key and NT accounts.

Contractors will conduct a security review and comply with MARCORSYSCOM 5239.2A, "WEB SITE ADMINISTRATION" prior to entering government information on a home page (contractor or government web page site). Copy of this order will be provided by the project officer under separate cover to the contractor.

All classified material received, generated, fabricated, or modified by this contract will be returned within 30 days after completion of contract or destroyed with destruction report being submitted to Commanding General, Marine Corps Systems Command (Attn: CMCC). Prior to any destruction of classified information a full listing of documents will be provided to the MARCORSYSCOM (CMCC) for review and approval. If additional contracting requirements exist where retention of classified information by the contractor facility is required, a written request to retain material for a period but not to exceed 2 years is required.

Block 10a. Contractor is authorized access to Government furnished cryptographic equipment and information. Access to COMSEC information, per NSA Manual 90-1, requires a final U.S. Government clearance and special briefings at the appropriate level. Subcontracting COMSEC information by a contractor requires prior approval from the Commanding General, MARCORSYSCOM (SECURITY).

Block 10j. The "For Official Use Only" information provided under this contract shall be safeguarded as specified in Attachment A.

Block 10K. Information on AIS personnel security program requirements for this contract are provided in Attachment B.

Block 11c. The contractor requires access to classified source data up to and including SECRET in support of this work effort. Any extracts or use of such data requires the contractor to apply derivative classification. Documentation generated as a result of this contract will be classified in accordance with source material provided by the user and will carry the most restrictive downgrading and/or declassification instructions, warning notices and control markings applicable. A listing of source material is to be included as a part of the document prepared by the contractor.

Use of cellular phones, hand-held radios, beepers and/or pagers, cordless telephones, and cordless microphones in a computer facility or Closed Area where classified processing is accomplished, requires special consideration.

Block 11d. The contractor is required to provide adequate storage for classified hardware to the level of Secret/COMSEC which will require 640 cubic feet that cannot be safeguarded in a regular- size approved storage container.

Block 11f. **The overseas activities required for this contract will be identified in the final contract.** These US government activities will be the locations for access to classified information. See Attachment C "Security Clauses for International Contracts" which provides information on how to protect classified material in foreign countries.

Block 11g. DTIC services required. DD Form 1540 will be prepared and processed in accordance with NISPOM, contracting activity will be involved in certifying need-to-know to DTIC. Information extracted from classified reference material shall be classified according to the markings on such material. The DD Form 1540 prepared under this contract shall be forwarded through Commanding General, MARCORSYSCOM (CTQ).

Block 11h. Communications Security (COMSEC) Supplement (DoD 5220.22-A) to the NISPOM for the handling of COMSEC material. Publishing or releasing of any COMSEC information by any means without written approval from the Department of Defense, National Security Agency, Fort George G. Meade, MD 20755-6000 via Commanding General, MARCORSYSCOM (MCSC) is PROHIBITED.

Contractor acquired/government furnished STE (Secure Terminal Device) is authorized to provide classified electronic mail and voice capability to support End Products. Transmission of classified data via STE and modems is authorized.

Item 17f will show MARCORSYSCOM (000) and (IC)

**CONTINUATION SHEETS FOR  
CONTRACT M67854-03-R-7041**

ATTACHMENT A  
PROCEDURES FOR "FOR OFFICIAL USE ONLY"

The following procedures will be used to protect FOR OFFICIAL USE ONLY (FOUO) information:

1. **HANDLING:** Access to FOUO material shall be limited to those employees who need the material to do their jobs. The FOR OFFICIAL USE ONLY marking is assigned to information when created by a DOD User Agency. FOR OFFICIAL USE ONLY is not a classification, but requires extra precautions to ensure it is not released to the public.
2. **MARKING:**
  - a. Mark an unclassified document containing FOUO information "FOR OFFICIAL USE ONLY" at the bottom of each page containing FOUO information and on the bottom of the front cover (if any) and on the back of the last page and on the back cover (if any).
  - b. In a classified document, mark:
    - An individual paragraph that contains FOUO, but not classified information, by placing "(FOUO)" at the beginning of the paragraph.
    - The top and bottom of each page that has both "FOR OFFICIAL USE ONLY" and classified information, with the highest security classification of information on that page.
    - "FOR OFFICIAL USE ONLY" at the bottom of each page that has FOUO but not classified.
    - If a classified document also contains FOUO information or if the classified material becomes FOUO when declassified, place the following statement on the bottom of the cover or the first page, under the classification marking: "NOTE: If declassified, review the document to make sure material is not FOUO and not exempt under Freedom of Information Act before public release."
  - c. Mark other records, such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so that the receiver or viewer knows the record contains FOUO information.
  - d. Mark each part of a message that contains FOUO information. Unclassified messages containing FOUO information must show the abbreviation "FOUO" before the text begins.
  - e. Make sure that documents, which transmit FOUO materials, call attention to any FOUO attachments.
  - f. Any FOUO material released to a contractor by a DOD User Agency must have the following statement on the front page or cover: THIS DOCUMENT CONTAINS INFORMATION EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT. EXEMPTION(S) APPLY.
3. **STORAGE:** To safeguard FOR OFFICIAL USE ONLY records during normal duty hours, place them in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the information. After normal duty hours, store FOUO records to prevent unauthorized access. File them with other unclassified records in unlocked files or desks when internal building security is provided. When there is no internal security, locked buildings or rooms usually provide adequate after-hours protection. For additional protection, store FOUO material in locked containers such as file cabinets, desks, or bookcases. Expenditure of funds for security containers or closed areas solely for the protection of FOUO data is prohibited.
4. **TRANSMISSION:** FOUO material shall be transported via first class mail, parcel post, or fourth class mail for bulk shipments. Transmit FOUO message traffic via approved secure communication system. Discussion of FOUO material over a secure telephone is authorized if necessary for performance of the contract. FOUO information shall be transmitted over telephone lines with encryption.
5. **RELEASE:** FOUO information shall not be released outside the contractor's facility except to representatives of the DOD but via the Government Contracting Officer.
6. **DESTRUCTION:** When no longer needed, FOUO information may be disposed of by any method, which will preclude its disclosure to unauthorized individuals.

**CONTINUATION SHEETS FOR  
CONTRACT M67854-03-R-7041**

ATTACHMENT "B"

AUTOMATED INFORMATION SYSTEMS (AIS)  
PERSONNEL SECURITY PROGRAM REQUIREMENTS

The U.S. Government conducts trustworthiness investigations of personnel who require access to unclassified information and who perform AIS duties. Requirements for these investigations are outlined in paragraphs 3-614, 3-710 and Appendix K of DoD 5200.2-R, available at <http://www.dtic.mil/whs/directives/>. Falsification of information submitted for any government-conducted investigation may result in contract default. The contractor shall include all of these requirements in any subcontracts involving AIS support.

Personnel performing work on AIS may be either a U.S. citizen or an Immigrant Alien (except as noted below). An Immigrant Alien is defined as a foreign national lawfully admitted to the United States for permanent residence. These personnel shall be designated as filling one of the three AIS Categories listed below. The Contracting Officer's Representative (COR) or Technical Representative (TR) shall determine if they or the contractor shall assign the AIS category to contractor personnel and inform the contractor of their determination. If it is decided the contractor shall make the assignment, the COR or TR must concur with the designation.

AIS Category I (High Risk) - may be filled by U.S. citizens only. Positions in which the incumbent is responsible for the planning, direction, and implementation of a computer security program; has a major responsibility for direction, planning, and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with relatively high risk for causing grave damage or realizing significant personal gain. Personnel whose duties meet the criteria for AIS Category I designation require a favorably adjudicated Single Scope Background Investigation (SSBI) or SSBI Periodic Reinvestigation (SSBI-PR), the updated standard for the BI listed in DoD 5200.2-R. The SSBI or SSBI-PR shall be updated every 5 years.

AIS Category II (Moderate Risk) - positions in which the incumbent is responsible for the direction, planning, design, operation or maintenance of a computer system, and whose work is technically reviewed by a higher authority at the AIS Category I level to insure the integrity of the system. Personnel whose duties meet the criteria for an AIS Category II designation require a favorably adjudicated National Agency Check (NAC), instead of the DNACI/NACI listed in DoD 5200.2-R.

AIS Category III - all other positions. Personnel whose duties meet the criteria for an AIS Category III designation require a favorably adjudicated NAC.

If an employee has a personnel security investigation at the appropriate level without a break in service for more than 24 months, with favorable adjudication, and in the case of AIS Category I is less than 5 years old, you do not need to submit an additional Electronic Personnel Security Questionnaire (EPSQ) for the trustworthiness determination. If required, the contractor will ensure personnel designated AIS category I, II, or III complete the EPSQ Standard Form (SF) 85P and provide it to their company's designated reviewer for and initial suitability determination. The reviewer will use the criteria outlined in Appendix G, SECNAVINST 5510.30A to make this initial determination. If, based on this initial review, the contractor gives the employee a negative trustworthiness determination the contractor will identify a replacement to the COR reviewer will submit their EPSQs to Defense Security Service (DSS). Investigative packages shall be submitted for all personnel in AIS Category I, II, or III prior to the employee being granted access to the AIS. Specific guidelines for obtaining software and submission of EPSQs are available at the DSS Web Site (www.dss.mil). If you are unfamiliar with the EPSQ SF85P, you may contact your local DSS office for further information.

Investigation results shall be returned to MARCORSYSCOM, Attn: Security, 2033 Barnett Ave., Quantico, VA 22134 for a trustworthiness determination. MARCORSYSCOM Quantico will notify the contractor of its decision. The contractor will promptly replace any individual for whom MARCORSYSCOM has communicated a negative trustworthiness determination.

The contractor will include the AIS Category for each person so designated on Visit Authorization Letters (VAL). VALs will be sent to the following address: Commanding General, MARCORSYSCOM, ATTN: Security, 2033 Barnett Ave., Quantico, VA 22134.

**CONTINUATION SHEETS FOR  
CONTRACT M67854-03-R-7041**

ATTACHMENT C  
SECURITY CLAUSES FOR INTERNATIONAL CONTRACTS

1. All classified information and material furnished or generated pursuant to this contract shall be protected as follows:
  - a. The recipient will not release the information or material to a third-country government, person, or firm without the prior approval of the releasing government.
  - b. The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government; and
  - c. The recipient will not use the information and material for other than the purpose for which it was furnished without the prior approval of the releasing government.
2. Classified information and material furnished or generated pursuant to this contract shall be transferred through government channels or other specified in writing by the Governments of the United States and Canada and only to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.
3. Classified information and material furnished under this contract will be remarked by the recipient with its government's equivalent security classification markings.
4. Classified information and material generated under this contract must be assigned a security classification as specified by the contract security classification specifications provided with this contract.
5. All cases in which it is known or there is reason to believe that classified information or material furnished or generated pursuant to this contract has been lost or disclosed to unauthorized persons shall be reported promptly and fully by the contract to its government's security authorities.
6. Classified information and material furnished or generated pursuant to this contract shall not be further provided to another potential contractor or subcontractor unless:
  - a. A potential contractor or subcontractor which is located in the United States or Canada has been approved for access to classified information and material by U.S. or Canadian security authorities; or
  - b. If located in a third country, prior written consent is obtained from the United States Government.
7. Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be returned to the U.S. contractor or be destroyed.
8. The recipient contractor shall insert terms that substantially conform to the language of these clauses, including this clause, in all subcontracts under this contract that involves access to classified information furnished or generated under this contract.