DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: SECRET

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

	a. PRIME CONTRACT NUMBER	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: PEO-STRI-14-W003	DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

X	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)*

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

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

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

7. SUBCONTRACTOR

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

8. ACTUAL PERFORMANCE

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

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Software, Networks, Information and Modeling & Simulation (SNIM). Provide R&D and AA&S services focused on enhancing the productivity of the Defense Research and Engineering community in performing their mission of ensuring that Warfighters today and tomorrow have superior and affordable technology to support their missions. Specific areas of focus include 1) Information Assurance, 2) Software Data Analysis, 3) Modeling & Simulation, and 4) Knowledge Management & Information Sharing.

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

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		X
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	X	
h. REQUIRE A COMSEC ACCOUNT	X	
i. HAVE TEMPEST REQUIREMENTS		X
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
l. OTHER *(Specify)*		X

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 [X] Through *(Specify)*

US Army PEO STRI (Public Affairs Office) and Contracting Officer Representative
12350 Research Parkway 12350 Research Parkway
Orlando, FL 32826-3276 Orlando, FL 32826-3276

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.)*

For Questions concerning this DD 254 please contact Stan Slupski at (407) 384-3540.

See item 13 Security Guidance Continued Sheet

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. [X] 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.)

See item 13 addendum

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. [ ] Yes [X] 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.)

The Government Project Manager's/Director's working in conjunction with the Contracting Officer of this effort will coordinate with the cognizant security office for the responsible for ensuring contractor compliance with the security terms of the DD FM 254 blocks 10,11,12,13 and addendum sheets. The government PM/PD's will verify and emphasize the contractor's security responsibilities during the life of the contract.

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 *(Include Area Code)*
Stanley Slupski	Security Specialist	(407) 384-3540

d. ADDRESS *(Include Zip Code)*	17. REQUIRED DISTRIBUTION	
PEO STRI ATTN: PEO STRI-SIO	[X]	a. CONTRACTOR
12350 Research Parkway	[ ]	b. SUBCONTRACTOR
Orlando, FL 32826-3276	[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
	[X]	f. OTHERS AS NECESSARY

ITEM 13 SECURITY GUIDANCE:

The following items apply to this contract.

GENERAL GUIDANCE:

1. The contractor and subcontractor(s) shall comply with the Security Agreement (DD Form 441) and Security Regulations (DoDM 5200.01 Volumes 1thru 4) DoD Information Security Program, (DoD 5220.22-M) National Industrial Security Program Operating Manual (NISPOM) current versions, AR 25-2, AR 380-67 and affiliated regulations.

2. The contractor's and subcontractor's employees requiring access to DOD government or DOD contractor's facilities where proof of a security clearance is required, the contractor and subcontractor(s) shall meet the security access requirements specified by the host and/or owner of those facilities.

3. The contractor and subcontractor(s) is/are not authorized to publically disclose or release SCI program information. Also the contractor and subcontractor(s) is/are not authorized to disclose or release collateral Classified Military Information (CMI) or Controlled Unclassified Information (CUI) pertaining to this contract, without prior review and approval from the government Public Affairs Officer, Contracting Officer, and cognizant security representative. Requests shall be submitted 14 working days in advance to the address specified in block 12.

4. The contractor and subcontractor(s) is/are required to protect Critical Program Information (CPI), and is not authorized to disclose or release any program Classified Military Information (CMI) or Controlled Unclassified Information (CUI) to Foreign Nationals without prior review and approval from the government Contracting Officer and cognizant security representative Foreign Disclosure Officer (FDO). Requests for disclosure or release shall be submitted 4 working weeks in advance to the address specified in block 12.

5. Prior to granting employees access to classified materials, the contractor and subcontractor(s) shall brief them with regard to their obligation to comply with the terms of the security regulations listed in paragraph 1. The contractor's and subcontractor(s) employees shall be debriefed when access to the material is terminated. A list of all employees who have had access to the classified information during the performance period of this Contract / Delivery Order shall be maintained by the company and be available for Defense Security Service (DSS) inspection.

6. The contractor may award subcontracts in furtherance of this effort. If access to classified information is required, the prime contractor is responsible to ensure compliance by the subcontractor for all security requirements. Copies of all subcontractor DD Forms 254 shall be forwarded to the Contracting Officer and the Cognizant Security Office at the address listed in block 16d.

7. Any Contractors/subcontractors owned by Foreign Companies and that have a clearance issued by the Defense Security Service under a Special Security Agreement need to have a National Interest Determination (NID) approved if access is required to: Top Secret; COMSEC; Restricted Data; SCI and/or SAP. NID requirements and justification must be sent through HQDA G2 to be forwarded to the approving agencies.

8. No security classification guide exists which is directly applicable to this effort. If, during this effort, it becomes necessary to create classified documentation for which there is no clear classification authority, the contractor shall notify the contract officer / contract monitor, who will seek the assistance and appropriate guidance from the local APM / PM milestone documents and project Security Office.

9. Contractors and their subcontractor(s) with security clearances shall comply with threat awareness training and reporting requirements per paragraph 1-14 of AR 381-12. Additionally the contractor shall report threat-related incidents, behavioral indicators to the Cognizant Security Office.

ITEM 10:

Ref Item 10.a: 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.

Ref Item 10.j: For Controlled Unclassified Information (CUI) which includes Official Use Only (FOUO) Information generated and/or provided under this contract shall be safeguarded and marked as specified in DoD 5200.01-V04.

ITEM 11:

Ref Item 11.c: The contractor requires access to classified source data up to and including ***(SECRET)*** 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.

Ref Item 11.d: Contractor must provide adequate storage and safeguards at their facility for classified hardware to the level of ***(SECRET)*** in accordance with security regulations listed in paragraph 1.

Ref Item 11.g: The contractor is authorized to use the services of Defense Technical Information Center (DTIC) and is required to prepare and process a DD Forms 1540 and 2345 to registration for Scientific and Technical Information Services. The contracting activity must be involved in certifying need-to-know to DTIC.

Ref Item 11.h: The contractor will coordinate administrative access to classified COMSEC material with the government program COMSEC custodian. The contractor will not receipt, copy, or generate classified COMSEC material. The contractor will maintain a current listing of all COMSEC accountable equipment and/or material associated with this contract to the government program COMSEC custodian. A copy of this listing will be filed with the contract DD 254.

Ref Item 11.j: The contractor shall develop, implement, and maintain a facility level OPSEC program to protect classified and sensitive unclassified information to be used at the contractor facility during the performance of this contract. The OPSEC requirements may be included in the Contractor's Standard Practice Procedures (SPP) or Technology Control Plan (TCP), whichever is more applicable.

Ref Item 11.k: This contract requires the use of the Defense Courier Service. The contracting activity will request DCS services from the Commander, Defense Courier Service, ATTN: Operations Division, Fort George G. Meade, MD 20755-5370."

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Contractor Generated, Communications Security (COMSEC) Material: any material generated by the contractor (including, but not limited to: correspondence, drawings, models, mockups, photographs, schematics, status programs and special inspection reports, engineering notes, computations and training aids) will be classified according to its own content and in accordance with AR380-5 and AR 380-40. Classification guidance will be taken from other elements of this Contract Security Classification Specification, DD Form 254, Government furnished equipment or data, or special instructions issued by the government program appointed COMSEC account manager (CAM), Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS:

1. Contractor employees or cleared commercial carriers shall not carry COMSEC materials on commercial passenger aircraft anywhere in the world without the approval of the government program appointed COMSEC account manager (CAM) or procuring contracting officer.

2. No contractor generated COMSEC or government furnished material may be provided to the Defense Technical Information Center (DTIC). Contractor generated technical reports will bear the statement **"Not Releasable to the Defense Technical Information Center per DOD Directive 5100-38."**

3. Classified COMSEC materials should be destroyed in the presence of the government program appointed COMSEC account manager (CAM) (primary and or alternate) and in accordance with AR 380-40, Safeguarding and Controlling Communications Security Material. Also, a record of the destruction must be recorded on Standard Form 153 rev (9-88) COMSEC Material Report and provided to the government program appointed COMSEC account manager (CAM) and contracts officer.

4. The following downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor must be done in accordance with AR 380-5 and AR 380-40.

5. All contractor personnel to be granted access to classified COMSEC information must be U.S. citizens granted FINAL clearance by the government prior to being given access. Immigrant aliens, interim cleared personnel, or personnel holding a contractor granted CONFIDENTIAL clearance are not eligible for access to classified COMSEC information released or generated under this contract without the express permission of the government program appointed COMSEC account manager (CAM) and Director, NSA.

6. Unclassified COMSEC Information released or generated under this contract shall be restricted in its dissemination to personnel involved in the contract. Release in open literature or exhibition of such information without express written permission of the Director, NSA is strictly prohibited.

7. Recipients of COMSEC Information under this contract may not release information to subcontractors without permission of the government program appointed COMSEC account manager (CAM) and User Agency.

8. Additional notices to be affixed to the cover and title or first page of contractor generated COMSEC documents:

a. "COMSEC MATERIAL – ACCESS BY CONTRACTOR PERSONNEL RESTRICTED TO U.S. CITIZENS HOLDING FINAL GOVERNMENT CLEARANCE."

b. "THIS PUBLICATION OR INFORMATION IT CONTAINS MAY NOT BE RELEASED TO FOREIGN NATIONALS WITHOUT PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA. ALL APPROVALS WILL IDENTIFY THE SPECIFIC INFORMATION AND COPIES OF THIS PUBLICATION AUTHORIZED FOR RELEASE TO SPECIFIC FOREIGN HOLDERS. ALL REQUESTS FOR ADDITIONAL ISSUANCES MUST RECEIVE PRIOR SPECIFIC APPROVAL FROM THE DIRECTOR, NSA"

9. Point of contact is the contract cognizant Security Office.

"FOR OFFICIAL USE ONLY" ATTACHMENT

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. Exemption 5 applies."

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.