

**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

TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED

SECRET

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

<input checked="" type="checkbox"/>	a. PRIME CONTRACT NUMBER N00178-05-D-4659-0003
<input type="checkbox"/>	b. SUBCONTRACT NUMBER
<input type="checkbox"/>	c. SOLICITATION OR OTHER NUMBER
	DUE DATE (YYMMDD)

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

<input checked="" type="checkbox"/>	a. ORIGINAL (Complete date in all cases)	DATE (YYMMDD) 4/26/2011
<input type="checkbox"/>	b. REVISED (Supersedes all previous specs)	Revision No. DATE (YYMMDD)
<input type="checkbox"/>	c. FINAL (Complete Item 5 in all cases)	DATE (YYMMDD)

4. THIS IS 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 KRATOS GOVERNMENT SOLUTIONS, INC 4820 EASTGATE MALL SAN DIEGO CA 92121-1977	b. CAGE CODE 0WJV2	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE (IOFWD) 11770 BERNARDO PLAZA COURT, SUITE 450 SAN DIEGO CA 92128-2426
--	------------------------------	---

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 KRATOS DEFENSE & SECURITY SOLUTIONS 17119 DAHLGREN ROAD KING GEORGE VA 22485	b. CAGE CODE 0P4N2	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip Code) DEFENSE SECURITY SERVICE (IOFCK2) 241 18TH STREET SUITE 100-A ARLINGTON VA 22202
--	------------------------------	--

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

This contract is providing engineering support and range services to NSWC/DD.

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

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the INSPOM 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):

Office of Naval Research
875 North Randolph Street Suite 1425/ Code 35 (Room 1127)
Arlington, VA 22203-1995

Task Order Manager, William J. Minter, NSWCCD, G24, 540 653-2358

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.)

National Industrial Security Program Operating Manual (NISPOM), dated February 2006 applies to this contract.
The contractor is not authorized to release any data to foreign nationals or foreign representatives without an approved export license.

The following will be provided by the TOM under separate correspondence:
Security Classification Guide, titled Naval Electromagnetic Launch (EML) Weapon Systems Security Classification Guide
OPNAV Instr 5513.3B Enc 148 (FOUO)

Security Classification Guide, titled U. S. Army Electromagnetic (EM) Gun Program Security Classification Guide dated 21 August 2006 (FOUO)

Security Classification Guide, titled Navstar Global Positioning System System Protection Guide dated 13 June 1997 (FOUO)

See attached continuation sheets for further guidance:

Continuation Sheet 1 is for all tasking except Rail Gun.
Continuation Sheet 2 is for Rail Gun an ONR sponsored program

William J. Minter G24 540 653-2358
Task Order Manager

Estimated completion date: 20160516

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to NISPOM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide any 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 BRENDA F. BENNETT	b. TITLE Contracting Officer's Security Rep	c. TELEPHONE (Include Area Code) 540 653-0463
--	---	---

d. ADDRESS (Include Zip Code)
Naval Surface Warfare Center, Dahlgren Division
6366 DOCK ROAD, SUITE 218, CX9
Dahlgren, VA 22448-5107

e. SIGNATURE
Brenda Bennett 4/26/2011

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 CONTRACTING OFFICER
 f. OTHERS AS NECESSARY

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Contractor Generated COMSEC Material: Any material generated by the contractor (including but not limited to: correspondence, drawings, models, mockups, photograph, schematics, status programs and special inspection reports, engineering notes, computation and training aids) will be classified according to its own content. 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 Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
2. No contractor generated 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 paper COMSEC material may be destroyed by burning, pulping or pulverizing. When a method other than burning is used, all residues must be reduced to pieces 5 mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
4. The following Downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2

DECLASSIFY ON: Source Marked "OADR" (If generated before 1 April 1995)

DATE OF SOURCE: (Date of document from which information is derived)

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 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 the 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 User Agency.
8. The requirements of DOD 5220-22-S are applicable to this effort.
9. 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 A 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."

PER SECNAV M-5510.36 OF JUN 2006

DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM

4-17 FOREIGN GOVERNMENT INFORMATION (FGI)

1. Information classified by a foreign government or international organization retains its original classification level or is assigned a U.S. classification equivalent to that provided by the originator to ensure adequate protection of the information (see exhibit 6C - Equivalent Foreign Security Classifications).

Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking if the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings. Authority to assign the U.S. classification equivalent does not require original classification authority.

2. Foreign Government Unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence shall be afforded a degree of protection that is at least equivalent to that required by the government or international organization that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including modified handling and transmission and allowing access by individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed a nondisclosure agreement. If the foreign protection requirement is

lower than the protection required for U.S. Confidential,
it
shall be marked in accordance with chapter 6, paragraph 6-
16. It
may be classified at a higher level if it meets the
criteria of
paragraph 4-2.

INFORMATION SHEET FOR CONTROL OF NATO MATERIAL

Ref: (a) OPNAVINST C5510.101D dtd 17 Aug 1982

1. Reference (a) states that the NATO Control Officers are responsible for control, protection, distribution and procurement of all NATO material for the serviced organization.
2. To ensure that this responsibility is fully met, it is necessary that all Center employees who acquire NATO material while in a travel status or attending meetings enter this material in to the accountability system immediately upon their return.
3. Material will be hand carried to code CX9, where required controls will be established. When there is no longer a need to retain NATO Secret material, it will be turned in (hand carried) to Code CX9 for destruction.
4. Reference (a) states the following procedures:
 - a. Cover letters for transmitting NATO documents will be given the highest classification of the document and marked, e.g., NATO (Classification) (Unclassified upon removal of enclosure).
 - b. U.S. documents that contain extracts from classified NATO documents will have the following statement written on the outside of the front cover (if any), on the first page, and the outside of the back cover (if any):

"THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION.
HANDLE IN ACCORDANCE WITH OPNAVINST C5510.101D."

In addition, each paragraph will be marked NATO Restricted (NR), NATO Confidential (NC), NATO Secret (NS), or COSMIC Top Secret (CTS) as appropriate.

- c. NATO Unclassified material shall be handled, transmitted, stored and destroyed as U.S. Unclassified and may be intermingled with U.S. material. It should be released only on a need-to-know basis. The custodian of the NATO Unclassified material may destroy the material by shredding.

d. NATO Restricted material will be handled as FOR OFFICIAL USE ONLY. It will be stored in filing cabinets, desks or other containers which are located in rooms where U.S. Government or Government-Contractor internal building security is provided during nonduty hours. Where such internal security is not available, locked buildings or rooms usually will provide adequate after hours protection. The custodian of NATO Restricted material may destroy the material with classified burn or by shredding.

e. NATO Confidential material is the equivalent of U.S. material with the same markings. It will be stored in safes, vaults or other security containers approved for U.S. documents of same classification; however, NATO documents shall be filed in separate folders and a distinct division between U.S. and NATO documents is required. The custodian of NATO Confidential material may destroy the material with classified burn or by shredding.

f. NATO Secret material is the equivalent of U.S. material with the same markings. It will be stored in safes, vaults or other security containers approved for U.S. documents of same classification; however, NATO Secret documents shall be filed in separate folders and a distinct division between U.S. and NATO documents is required. Receipts and logs are maintained on the receipt, disposition and dispatch of NATO Secret material. All NATO Secret material is controlled by the NATO Control Officer. The custodian of NATO Secret material will be required to sign for NATO Secret from the NATO Control Office. Custodians of NATO Secret material will be required to conduct an annual inventory of their holdings. All NATO Secret material is to be returned to the NATO Control Officer for destruction.

g. To request a NATO document, the short title, originator, and date of the document must be provided to NSWC Security Office.

FOR OFFICIAL USE ONLY (FOUO ADDENDUM)

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

1. **HANDLING:** Access to FOUO material shall be limited to those employees needing the material to do their jobs. The FOUO marking is assigned to material created by a DoD user agency. FOUO is not a classification, but requires extra precaution to insure it is not released to the public.
2. **MARKING:** Mark unclassified documents containing FOUO "FOR OFFICIAL USE ONLY" at the bottom of each page and the back cover (if any). In a classified document, mark:
 - a. An individual paragraph that contains FOUO, but not classified material, by placing "FOUO" at the beginning of the paragraph.
 - b. The top and bottom of each page that has both FOUO and classified material with the highest security classification of the material on that page.
 - c. "FOUO" at the bottom of each page that has FOUO but not classified material.
 - d. If a classified document also contains FOUO material 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 before public release."
 - e. Mark other records such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so the receiver or viewer know the record contains FOUO material.
 - f. Mark each part of a message that contains FOUO material. Unclassified messages containing FOUO material must show the abbreviation "FOUO" before the text begins.
 - g. Insure documents that transmit FOUO material call attention to any FOUO attachments.
 - h. 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 MATERIAL EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT."
3. **FOUO STORAGE:** During normal duty hours, place FOUO material in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the material. After normal duty hours, store FOUO material to prevent unauthorized access. File with other unclassified records in unlocked files or desk when internal building security is provided. When there is not 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, desk or bookcases. Expenditure of funds for security container solely for the protection of FOUO material is prohibited.
4. **TRANSMISSION:** FOUO material shall be transmitted via U.S. Postal Service First Class mail or standard mail for bulk shipments. Electronic transmissions of FOUO information (i.e. voice, data, facsimile) shall be by approved secure communications system whenever practical. All means used shall preclude unauthorized public disclosure.
5. **RELEASE:** FOUO information may be disseminated within the DoD components and between officials of the DoD components, cleared DoD contractors, consultants, and grantees in the conduct of official business for the DoD and DON provided that dissemination is not further controlled by a distribution statements (per NAVSEA M-5510.36 Jun 2006).
6. **DESTRUCTION:** When no longer needed, FOUO material shall be disposed of by a method that precludes its disclosure to unauthorized individuals.

AUGUST 2009

CONTINUATION SHEET - DD FORM 254

All reports containing scientific/technical information (both classified and unclassified) will be marked on both the cover and title page with the following distribution statement: (For Intelligence Data - See Statement Below)*:

"Distribution authorized to U.S. GOVERNMENT AGENCIES ONLY; TEST AND EVALUATION". Other requests for this document must be referred to Commander, Dahlgren Division, Naval Surface Warfare Center, Code G24, Dahlgren, VA 22448-5100.

*Intelligence data reports - distribution statement as follows: "FURTHER DISSEMINATION ONLY AS DIRECTED BY COMMANDER, DAHLGREN DIVISION, NAVAL SURFACE WARFARE CENTER (CODE CX10), DAHLGREN, VA 22448-5100 OR THE OFFICE OF NAVAL INTELLIGENCE (ONI-52)".

All technical data provided to the contractor by the government will be protected from public disclosure in accordance with the markings contained thereon. All other information relating to the items to be delivered or services to be performed under this contract may not be disclosed by any means without prior approval of the authorized representative of the contracting officer. Dissemination or public disclosure includes, but is not limited to, permitting access to such information by foreign nationals or by any other person or entity; publication of technical or scientific papers; advertising; or any other proposed public release. The contractor shall provide adequate physical protection to such information as to preclude access by any person or entity not authorized such access by the government.

Due to the sensitivity of this program, no classified material received or generated under this contract will be transferred to any other contractor or agency without the approval of the Contracting Officer or Contracting Officer's Representative (COR). For intelligence data reports see the intelligence supplement.

Information on this contract is not releasable to personnel possessing reciprocal clearances without the written approval of NSWCDD. For intelligence data reports see the intelligence supplement.

All visit requests for contractor personnel visiting NSWCDL shall be sent through the Joint Personnel Adjudication System (JPAS), under SMO code 00178.

Visit requests for Contractor Personnel not submitted via JPAS shall be faxed to the Information and Personnel Security Office (540-653-4372) no later than five (5) working days prior to the intended visit. All visit requests not submitted via JPAS shall have "NEED-TO-KNOW" certified by the individual identified in Item 13 (COR, TPOC, TOM). All requests shall contain the information required by Chapter 6, NISPOM, and shall not exceed 12 months.

Visit requests for subcontractors to activities other than Intelligence Community (IC) activities will have "NEED-TO-KNOW" certified by the prime contractor. Visit requests to IC activities shall be on a case-by-case basis and determined by the IC.

Any material produced under the terms of this contract will be classified directly from the source document(s) from which it was obtained. It will be marked with the most restrictive downgrading/declassification statement contained in such documents.

INTELLIGENCE INFORMATION

Intelligence information required in connection with performance shall be acquired under the direction of the Dahlgren Division, Naval Surface Warfare Center (NSWCDD) Technical Intelligence Office (TIO), Code W14. Foreign intelligence will be provided in accordance with DOD Directive, DOD-0000-151C-95, DODIPP Production Procedures; OPNAV Instructions 3880.6 and 3811.1C and NSWCDD Instructions 3880.6A and 3811.1C.

The following conditions of release apply to Foreign Intelligence information.

a. The material does not become the property of the contractor and may be withdrawn at any time. Upon expiration of the contract, all foreign intelligence released and any material using data from such intelligence shall be returned to the NSWCDD Senior Intelligence Officer (SIO) for final disposition. Only with the prior authorization of the Office of Naval Intelligence (ONI-52) via the NSWCDD SIO may the contractor retain such material.

b. The contractor shall not release the foreign intelligence material to any activity or person of the contractors organization not directly engaged in providing services under the contract or to another contractor (including subcontractors), government agency, private individual, or organization without prior approval of the NSWCDD SIO, or ONI-52 via the NSWCDD SIO.

c. Intelligence material shall not be released to foreign nationals or immigrant aliens who may be employed by the contractor, regardless of the level of their security clearance or access authorization, without the prior approval of ONI-52 via the NSWCDD SIO.

d. Intelligence material shall not be reproduced without prior approval of the NSWCDD SIO, or ONI-52 via the NSWCDD SIO. All intelligence material shall bear a prohibition against reproduction while in the custody of the contractor.

CONTINUATION SHEET - DD FORM 254

e. The contractor shall maintain records which contain the names of all individuals granted access to foreign intelligence material in the contractor's custody. These records shall be furnished to the NSWCDD Contracting Officer or the NSWCDD SIO on demand. The contractor shall ensure all individuals granted access to foreign intelligence information are aware of and abide by the controls set forth above.

Foreign intelligence is defined in SECNAVINST 5510.36 as the product from the collection, evaluation, analysis, integration, and interpretation of intelligence information about a foreign power and which is significant to the national security, foreign relations, or economic interests of the U.S. and which is provided by a Government agency that is assigned an intelligence mission.

CONTINUATION SHEET 2 – DD FORM 254

1. Contractor-prepared documents containing scientific or technical information (classified or unclassified) shall be marked on the cover, title page, and Report Documentation Page (if present) with the following:

DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (Critical Technology) (19 May 2005). Other requests shall be referred to the Office of Naval Research, ONR 352, 875 N. Randolph St., Room 1127, Arlington, VA 22203-1995.

WARNING – This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50, U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

Destruction Notice - For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document. Classified information, destroy in accordance with DoD 5220.22-M (National Industrial Security Program Operating Manual) or SECNAVINST 5510.36 (Information Security Program (ISP) Regulation).

The above supersedes the distribution statement requirements stated in the Security Classification Guides referenced in Block 13 of the DD 254.

2. Information regarding this contract or any program related to the contract shall be disclosed in accordance with NISPOM (DoD 5220.22-M) Chapter 5, Section 5. (Subjects addressed in the section include disclosure of classified and unclassified information to employees, subcontractors, DoD activities, Federal agencies, foreign persons, other contractors, and the public.) All information for public release shall be approved by the activity identified in block 12 of the DD 254.

The above supersedes the public release requirements stated in the Security Classification Guides referenced in Block 13 of the DD 254.

3. The contractor shall inform NCIS and the COR:
 - a. Of inquiries regarding this contract or any program related to the contract, even apparently innocent ones, received from foreign sources.
 - b. At least 30 days in advance, of contractor participation in foreign technical conferences related to this contract or any program related to the contract.
 - c. Of detected electronic intrusion attempts at the contractor.

These requirements are in addition to the reporting requirements stated in DoD 5220.22-M.

CONTINUATION SHEET 2 – DD FORM 254

4. Export-controlled unclassified technical information related to this contract shall be transmitted between facilities by:
- a. Sending the information over a local area network (if available) connecting the facilities,
 - b. Posting the information on and downloading it from railgun VIEWNet,
 - c. Mailing encrypted storage media containing the information (see item 5), or
 - d. Sending the information via SIPRNet.

Transmittal by unclassified email or via FTP sites other than VIEWNet is prohibited.

5. Export-controlled unclassified technical information related to this contract shall be encrypted using a NIST FIPS PUB 140-2 or 140-3 validated method whenever the information is:
- a. Stored on a computer that is connected, directly or indirectly (e.g. via a LAN, server, and firewall), to the Internet.
 - b. Stored on a device (e.g. laptop computer, flash drive, compact disc) that is located in a space that is not certified for storage of DoD Confidential or higher, or DoE L or Q, materials.
6. Controlled unclassified information shall not be stored on or loaded onto laptop computers, personal digital assistants, electronic storage devices, compact disks and similar portable electronic computing and communication devices used on foreign travel. U.S. and foreign laws regarding export of technical information shall be complied with.
7. The contractor shall provide an open-storage area cleared to the SECRET level. The open-storage area shall have a restricted-access, daily use, dedicated work space leased to the government for use by approved, cleared government customers and contractors. In addition, the workspace shall include classified computer processing and printing capabilities, SIPRNET communication capability, and a STU-III telephone system.

ADDITIONAL SECURITY GUIDELINES FOR COMSEC

Contractor Generated COMSEC Material: Any material generated by the contractor (including but not limited to: correspondence, drawings, models, mockups, photograph, schematics, status programs and special inspection reports, engineering notes, computation and training aids) will be classified according to its own content. 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 Contracting Officer, or his/her duly appointed representative.

REQUIREMENTS

1. Contractor employees or cleared commercial carriers shall not carry classified COMSEC material on commercial passenger aircraft anywhere in the world without the approval of the procuring contracting officer.
2. No contractor generated 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 paper COMSEC material may be destroyed by burning, pulping or pulverizing. When a method other than burning is used, all residues must be reduced to pieces 5 mm or smaller in any dimension. When classified COMSEC material other than paper is to be destroyed, specific guidance must be obtained from the User Agency.
4. The following Downgrading and Declassification notation applies to all classified COMSEC information provided to and generated by the contractor:

DERIVED FROM: NSA/CSSM-123-2

DECLASSIFY ON: Source Marked "OADR" (If generated before 1 April 1995)

DATE OF SOURCE: (Date of document from which information is derived)

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 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 the 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 User Agency.
8. The requirements of DOD 5220-22-S are applicable to this effort.
9. 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 A 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."

PER SECNAV M-5510.36 OF JUN 2006

DEPARTMENT OF THE NAVY INFORMATION SECURITY PROGRAM

4-17 FOREIGN GOVERNMENT INFORMATION (FGI)

1. Information classified by a foreign government or international organization retains its original classification level or is assigned a U.S. classification equivalent to that provided by the originator to ensure adequate protection of the information (see exhibit 6C - Equivalent Foreign Security Classifications).

Foreign government information retaining its original classification markings need not be assigned a U.S. classification marking if the responsible agency determines that the foreign government markings are adequate to meet the purposes served by U.S. classification markings. Authority to assign the U.S. classification equivalent does not require original classification authority.

2. Foreign Government Unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both are to be held in confidence shall be afforded a degree of protection that is at least equivalent to that required by the government or international organization that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to U.S. Confidential information, including modified handling and transmission and allowing access by individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed a nondisclosure agreement. If the foreign protection requirement is

lower than the protection required for U.S. Confidential,
it
shall be marked in accordance with chapter 6, paragraph 6-
16. It
may be classified at a higher level if it meets the
criteria of
paragraph 4-2.

FOR OFFICIAL USE ONLY (FOUO ADDENDUM)

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

1. **HANDLING:** Access to FOUO material shall be limited to those employees needing the material to do their jobs. The FOUO marking is assigned to material created by a DoD user agency. FOUO is not a classification, but requires extra precaution to insure it is not released to the public.
2. **MARKING:** Mark unclassified documents containing FOUO "FOR OFFICIAL USE ONLY" at the bottom of each page and the back cover (if any). In a classified document, mark:
 - a. An individual paragraph that contains FOUO, but not classified material, by placing "FOUO" at the beginning of the paragraph.
 - b. The top and bottom of each page that has both FOUO and classified material with the highest security classification of the material on that page.
 - c. "FOUO" at the bottom of each page that has FOUO but not classified material.
 - d. If a classified document also contains FOUO material 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 before public release."
 - e. Mark other records such as computer print outs, photographs, films, tapes, or slides "FOR OFFICIAL USE ONLY" so the receiver or viewer know the record contains FOUO material.
 - f. Mark each part of a message that contains FOUO material. Unclassified messages containing FOUO material must show the abbreviation "FOUO" before the text begins.
 - g. Insure documents that transmit FOUO material call attention to any FOUO attachments.
 - h. 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 MATERIAL EXEMPT FROM MANDATORY DISCLOSURE UNDER THE FREEDOM OF INFORMATION ACT."
3. **FOUO STORAGE:** During normal duty hours, place FOUO material in an out-of-sight location if your work area is accessible to persons who do not have a valid need for the material. After normal duty hours, store FOUO material to prevent unauthorized access. File with other unclassified records in unlocked files or desk when internal building security is provided. When there is not 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, desk or bookcases. Expenditure of funds for security container solely for the protection of FOUO material is prohibited.
4. **TRANSMISSION:** FOUO material shall be transmitted via U.S. Postal Service First Class mail or standard mail for bulk shipments. Electronic transmissions of FOUO information (i.e. voice, data, facsimile) shall be by approved secure communications system whenever practical. All means used shall preclude unauthorized public disclosure.
5. **RELEASE:** FOUO information may be disseminated within the DoD components and between officials of the DoD components, cleared DoD contractors, consultants, and grantees in the conduct of official business for the DoD and DON provided that dissemination is not further controlled by a distribution statements (per NAVSEA M-5510.36 Jun 2006).
6. **DESTRUCTION:** When no longer needed, FOUO material shall be disposed of by a method that precludes its disclosure to unauthorized individuals.

AUGUST 2009

INFORMATION SHEET FOR CONTROL OF NATO MATERIAL

Ref: (a) OPNAVINST C5510.101D dtd 17 Aug 1982

1. Reference (a) states that the NATO Control Officers are responsible for control, protection, distribution and procurement of all NATO material for the serviced organization.
2. To ensure that this responsibility is fully met, it is necessary that all Center employees who acquire NATO material while in a travel status or attending meetings enter this material in to the accountability system immediately upon their return.
3. Material will be hand carried to code CX9, where required controls will be established. When there is no longer a need to retain NATO Secret material, it will be turned in (hand carried) to Code CX9 for destruction.

4. Reference (a) states the following procedures:

a. Cover letters for transmitting NATO documents will be given the highest classification of the document and marked, e.g., NATO (Classification) (Unclassified upon removal of enclosure).

b. U.S. documents that contain extracts from classified NATO documents will have the following statement written on the outside of the front cover (if any), on the first page, and the outside of the back cover (if any):

“THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION.
HANDLE IN ACCORDANCE WITH OPNAVINST C5510.101D.”

In addition, each paragraph will be marked NATO Restricted (NR), NATO Confidential (NC), NATO Secret (NS), or COSMIC Top Secret (CTS) as appropriate.

c. NATO Unclassified material shall be handled, transmitted, stored and destroyed as U.S. Unclassified and may be intermingled with U.S. material. It should be released only on a need-to-know basis. The custodian of the NATO Unclassified material may destroy the material by shredding.

d. NATO Restricted material will be handled as FOR OFFICIAL USE ONLY. It will be stored in filing cabinets, desks or other containers which are located in rooms where U.S. Government or Government-Contractor internal building security is provided during nonduty hours. Where such internal security is not available, locked buildings or rooms usually will provide adequate after hours protection. The custodian of NATO Restricted material may destroy the material with classified burn or by shredding.

e. NATO Confidential material is the equivalent of U.S. material with the same markings. It will be stored in safes, vaults or other security containers approved for U.S. documents of same classification; however, NATO documents shall be filed in separate folders and a distinct division between U.S. and NATO documents is required. The custodian of NATO Confidential material may destroy the material with classified burn or by shredding.

f. NATO Secret material is the equivalent of U.S. material with the same markings. It will be stored in safes, vaults or other security containers approved for U.S. documents of same classification; however, NATO Secret documents shall be filed in separate folders and a distinct division between U.S. and NATO documents is required. Receipts and logs are maintained on the receipt, disposition and dispatch of NATO Secret material. All NATO Secret material is controlled by the NATO Control Officer. The custodian of NATO Secret material will be required to sign for NATO Secret from the NATO Control Office. Custodians of NATO Secret material will be required to conduct an annual inventory of their holdings. All NATO Secret material is to be returned to the NATO Control Officer for destruction.

g. To request a NATO document, the short title, originator, and date of the document must be provided to NSWC Security Office.