

<b>DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION</b>  <i>(The requirements of the DoD National Industrial Security Program Operating Manual apply to all security aspects of this effort.)</i>				1. CLEARANCE AND SAFEGUARDING	
				a. FACILITY CLEARANCE REQUIRED <b>TOP SECRET</b>	
				b. LEVEL OF SAFEGUARDING REQUIRED <b>TOP SECRET</b>	
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)	20040908
b. SUBCONTRACT NUMBER			b. REVISED <i>(Supersede all previous specs)</i>	Revision Number	DATE (YYYYMMDD)
c. SOLICITATION OR OTHER NUMBER	DUE DATE (YYYYMMDD)		c. FINAL <i>(Complete Item 3 in all cases)</i>	DATE (YYYYMMDD)	
<b>X</b>	<b>N00421-04-R-0088</b>				
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. <i>If YES, complete the following:</i>					
Classified material received or generated under _____ (preceding contract number) is transferred to this follow-on contract.					
5. IS THIS A FINAL DD FORM 254? <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO. <i>If YES, complete the following:</i>					
In response to the contractor's request dated _____ retention of the identified 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>FOR BIDDING PURPOSES ONLY NOT VALID FOR ACTUAL CONTRACT</b>		b. CAGE CODE <b>N/A</b>	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> <b>N/A</b>		
7. SUBCONTRACTOR					
a. NAME, ADDRESS, AND ZIP CODE <b>N/A</b>		b. CAGE CODE <b>N/A</b>	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> <b>N/A</b>		
8. ACTUAL PERFORMANCE					
a. LOCATION <b>N/A</b>		b. CAGE CODE <b>N/A</b>	c. COGNIZANT SECURITY OFFICE <i>(Name, Address, and Zip Code)</i> <b>N/A</b>		
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT <b>Naval Air Systems Command (NAVAIR) Warfare Analysis Department, AIR 4.10 Support COR: Gordon K. Smith, 4.10.1.2, (301) 995-7643. TPOC: Dave Tauras, 4.10.1.2, (301) 342-0179.</b>					
10. THIS CONTRACT WILL REQUIRE ACCESS TO:			11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:		
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	YES <input checked="" type="checkbox"/>	NO <input type="checkbox"/>	a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	YES <input type="checkbox"/>	NO <input checked="" type="checkbox"/>
b. RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>
d. FORMERLY RESTRICTED DATA	<input type="checkbox"/>	<input checked="" type="checkbox"/>	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	<input type="checkbox"/>	<input checked="" type="checkbox"/>
e. INTELLIGENCE INFORMATION:			e. PERFORM SERVICES ONLY	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(1) SENSITIVE COMPARTMENT INFORMATION (SCI)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES	<input type="checkbox"/>	<input checked="" type="checkbox"/>
(2) NON-SCI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER	<input checked="" type="checkbox"/>	<input type="checkbox"/>
f. SPECIAL ACCESS INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	h. REQUIRE A COMSEC ACCOUNT	<input checked="" type="checkbox"/>	<input type="checkbox"/>
g. NATO INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	i. HAVE TEMPEST REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
h. FOREIGN GOVERNMENT INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
i. LIMITED DISEMINATION INFORMATION	<input type="checkbox"/>	<input checked="" type="checkbox"/>	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	<input checked="" type="checkbox"/>	<input type="checkbox"/>
j. FOR OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/>	<input type="checkbox"/>	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):

**Commanding Officer, NAWCAD/NAS PAO, Unit NASAD, Bldg. 409, 22268 Cedar Point Road, Patuxent River, MD 20670-1154, 301-342-7710**

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.)

**10a. A final U.S. Government clearance, at the appropriate level, is required prior to COMSEC access.** Written approval of the Contracting Officer is required prior to subcontracting.

**10a(2):** Contract requires access to intelligence data, including the SIPRNET, as certified by the COR via the NAVAIR/NAWCAD STILO. The contractor shall not intentionally access, download, or further disseminate intelligence data without the guidance and permission of the NAVAIR/NAWCAD STILO. Contractor shall comply with Naval Air Warfare Center Aircraft Division Scientific and Technical Intelligence Liaison Officer memo of 01 JUN 99 (attached). Written approval of the User Agency Contracting Officer is required prior to subcontracting.

Reviewed by: *Stephen Hendricks*  
 Senior Intelligence Officer: Stephen Hendricks

**10g:** There is no valid requirement for NATO access, however inadvertent access may occur because NATO information is available on the SIPRNET. A final U.S. Government clearance, at the appropriate level, is required for access to NATO information. Written approval of the Contracting Officer is required prior to subcontracting.

**10j:** For Official Use Only Information (FOUO) generated and/or provided under this contract shall be safeguarded and marked as specified in DoD 5400.7-R, Chapters 3 and 4 (attached).

The contractor shall comply with the requirements of the Information Systems Security Programs as described in NAVAIRWARCENACCDIVINST 5239.1. All systems, regardless of the level of data processed, will be accredited in accordance with the above instructions.

**11c:** Contractor will be generating classified and unclassified technical documents at Contractor facilities. The Government will be responsible for classification guidance and markings, distribution statements, and declassification instructions on those documents. For further guidance contact the COR/TPOC listed in block 9. The COR/TPOC is responsible for ensuring that distribution statements are applied to all classified and unclassified technical documents in accordance with SECNAVINST 5510.36, Chapter 8.

**11g:** The contractor will be required to prepare and process DD Form 1540 (attached) prior to requesting DTIC services.

**11h:** 10a. A final U.S. Government clearance, at the appropriate level, is required prior to COMSEC access. Written approval of the Contracting Officer is required prior to subcontracting.

**11i:** Contractors operating contractor-owned or controlled Information Technology Resources on non-Government premises to provide classified computer support to the DON, in addition to the requirements of the NISPOM, must submit a TEMPEST Requirements Questionnaire for Contractor Facilities (attached) for systems processing data at the SECRET Special Category level or above within 30 days of contract award.

**11j:** 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. Contract data requirements list (CDRL) and data item description (DID) attached. The OPSEC plan shall be submitted to the NAVAIR within 90 days of contract award for acceptance and approval. Contractor shall mail preliminary draft OPSEC Plan in MS Word 6.0 (or later) on Compact Disc and hard copy to: Commander, Attn: 7.4.3, B463 Unit 10, 22514 McCoy Road, Patuxent River, MD 20670-1457. Final plan, due 45 days after Government approval (NAWCAD 7.4.3) of draft. While performing aboard NAVAIR sites, the contractor shall comply with the provisions of NAWCADINST 3432.1A; at all other sites, the contractor shall comply with the local command and/or program OPSEC plan.

**11k:** The contractor shall require the use of Defense Courier Service for delivery of all COMSEC and Top Secret Information.

**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 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

See item 13 above

**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

NONE

**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 MARK A. DAVIS	b. TITLE CONTRACTING OFFICER'S SECURITY REPRESENTATIVE (COSR)	c. TELEPHONE (include Area Code) 301-342-8045
---	--	--

d. ADDRESS (include Zip Code)  
 Commander, Naval Air Warfare Center-Aircraft Division  
 Attn: 7.4.1, Bldg. 2185, Suite 1232, 22347 Cedar Point Road  
 Patuxent River, MD 20760-1161

**17. REQUIRED DISTRIBUTION**

<input checked="" type="checkbox"/>	a. CONTRACTOR
<input checked="" 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 type="checkbox"/>	e. ADMINISTRATIVE CONTRACTING OFFICER
<input checked="" type="checkbox"/>	f. OTHERS AS NECESSARY

**e. SIGNATURE** *Mark A. Davis* 9/9/04

**COR, COSR**

3800  
AIR-4.10.4  
1 JUN 1999

MEMORANDUM

From: Scientific and Technical Intelligence Liaison Officer, 48150 Shaw Road Unit 5, Suite S220,  
Patuxent River, Maryland 20670-1907

To: Distribution

Subj: POLICY GOVERNING RELEASE OF INTELLIGENCE TO CONTRACTORS

Encl: (1) Request for Access/Release of Intelligence to Contractors, dated 1 June 1999

Ref: (a) DCID 1/7 Security Controls on the Dissemination of Intelligence Information  
(b) SECNAVINST 5510.36

1. As directed by reference (a), policy and procedures governing the release of intelligence to contractors and consultants is as follows:

- a. The Senior Officials of the Intelligence Community (SOIC's), defined by reference (a), designate the Contracting Officer's Representative (COR) and STILO, the local intelligence program manager, as the official approving authorities for **release of intelligence information** to appropriately cleared or access-approved US contractors and consultants (hereinafter "contractor") having a demonstrated "NEED TO KNOW" without referral to the originating agency prior to release provided that:
  - (1) At the initiation of the contract, the COR **specifies AND certifies in writing via the STILO** that disclosure of the specified information does not create an unfair competitive advantage for the contractor or a conflict of interest with the contractor's obligation to protect the information. **If, during the course of the contract, the contractor's requirements for information changes to require new or significantly different information, the COR shall make a new specification and certification.** In cases where the designated official cannot or does not resolve the issue of unfair competitive advantage or conflict of interest, the STILO will seek to obtain consent of the originator for release.
  - (2) Release is only made to contractors certified by the COR via the STILO as performing classified services in support of a national security mission.
  - (3) The contractor has an approved safeguarding capability if retention of the intelligence is required.
  - (4) **Contractors are not authorized to disclose further or release intelligence to any of their components or employees or to another contractor (including subcontractors) without the prior written notification and approval of the STILO unless such disclosure or release is authorized in writing at the initiation of the contract as an operational requirement.**
  - (5) Intelligence released to contractors, all reproductions thereof, and all other material generated based on, or incorporating data therefrom (including authorized reproductions), remain the property of the US Government. Final disposition of the intelligence information shall be governed by the STILO.
- b. The guidance for contractors inside a government owned or controlled facility are listed in paragraph 1.a.

c. The policies and procedures for contractors outside government owned or controlled facilities are listed in paragraph 1.a. with the following additional policies and procedures:

- (1) The STILO is responsible for ensuring that releases to contractors of intelligence marked ORCON and /or PROPIN are made only with the consent of the originating agency pursuant to reference (a).
- (2) The STILO shall maintain a record of material released.
- (3) Contractors shall establish procedures to control all intelligence received, produced, and held by them in accordance with the provisions of the National Industrial Security Program Operating Manual. This will not impose internal receipt and document accountability requirements for the internal traceability and audit purposes.
- (4) All reproductions and extractions of intelligence shall be classified, marked, and controlled in the same manner as the original(s).
- (5) Sensitive Compartmented Information released to contractors shall be controlled pursuant to the provisions of DCID 1/19, Security Policy for Sensitive Compartmented Information (SCI).
- (6) The STILO shall delete any reference to the Central Intelligence Agency, the phrase "Directorate of Operations" and any of its components, the place acquired, the field number, the source description, and the field dissemination from all CIA Directorate of Operations reports passed to contractors, unless prior approval to do otherwise is obtained from CIA.

2. Enclosure (1) is the form letter that is to be completed and signed by the COR or Technical Point of Contact (TPOC) and validated by the STILO for a description of the intelligence information required for the contractor to perform the task. **NEED-TO-KNOW IS STILL THE DETERMINING BASIS FOR ACCESS.** The original release form will be maintained by the STILO office with the DD254 that is currently on file and a copy will be returned to the COR or TPOC.

3. Enclosure (2) is a list of intelligence producers; it should assist you in determining if the information that is to be released to a contractor could be considered intelligence. There will be exceptions to this list; if the information appears to be "threat" related or involves a foreign government's platforms/systems and you are still unsure, call the STILO office and they can assist you in making a determination.

4. Questions or comments should be directed to the NAVAIR STILO, Mr. Steve Hendricks at commercial (301) 342-6320 or DSN 342-6320 or the following STILO personnel:

Mrs. Kris Dennie-Young, 342-6310

Mr. Jim Kelly, 342-6323

Mrs. Jeanne Hall, 342-6315



STEPHEN K. HENDRICKS

Distribution to all government contract representatives listed below initiating contract DD254's requiring access to Intelligence Information:

Contracting Officer's Representatives (COR's)

Technical Points-of-Contact (TPOC's)

Contracting Officer's Security Representatives (COSR's)

**REQUEST FOR ACCESS/RELEASE OF INTELLIGENCE TO CONTRACTORS**

(Revised copy 1 June 1999 - previous form is now obsolete)

IAW DCID 1/7 "Security Controls on the Dissemination of Intelligence Information" of 30 June 1998, Request the following intelligence information be approved for access/release to:

\_\_\_\_\_ under Contract \_\_\_\_\_  
Company Name Contract Number and D.O. if applicable

Description of technical intelligence information required (please be as specific as possible):

As a Senior Official of the Intelligence Community (SOIC) designated representative for the Naval Air Systems Command or the Naval Air Warfare Center Aircraft Division Patuxent River, I hereby certify that access/release of the intelligence product listed above will in no way give the contractor an unfair competitive advantage or create a conflict of interest AND the contractor has a NEED-TO-KNOW and proper clearances supported by the DD254 and Scope of Work stated in this contract. \*\*

\_\_\_\_\_  
**Contracting Officer's Representative (COR)**

Name printed/typed, date and signature

or

\_\_\_\_\_  
**Contract Technical Point of Contact**

Name printed/typed, date and signature

**Validation by STILO:**

\_\_\_\_\_  
Name printed/typed, date and signature

\*\* In the event that the COR or TPOC cannot determine whether the information would give the contractor an unfair competitive advantage or create a conflict of interest, the request will be referred by the STILO to the originating organization for resolution.

Enclosure (1)

**TEMPEST REQUIREMENTS QUESTIONNAIRE**  
**(FOR NAVY AND MARINE CORPS FACILITIES)**

1. Should the criteria of enclosure (1) to OPNAVNOTE C5510 apply, provide the following requested data (TEMPEST Requirements Questionnaire) and submit to:

COMMANDING OFFICER  
SPAWAR SYSTEMS CENTER CHARLESTON  
CODE 723  
PO BOX 190022  
NORTH CHARLESTON SC 29419-9022

2. Provide the name, address, position title, and phone number (at the facility where classified processing will occur) of a point of contact who is knowledgeable of the processing requirements, the types of equipment to be used, and the physical layout of the facility.

3. Provide the specific geographical location (address and zip code) where classified processing will be performed.

4. What are the classification levels of material to be processed/handled by electronic or electromechanical information systems and what percentage is processed at each level?

5. What special categories of classified information are processed?

6. Is there a direct connection (wireline or fiber) to a Radio Frequency (RF) transmitter(s) located either locally or at a remote site?

7. Are there any RF transmitters located within 6 meters of the system processing National Security Information or the system's RED signal lines?

8. Describe how access is controlled to your facility including the building, compound, plant, property, and/or parking lots. Where are visitors first challenged/identified? Include controls such as alarms, guards, patrols, fences, and warning signs. Provide a simple layout of the facility and adjacent uncontrolled areas.

9. Are there other tenants in the building who are not U.S. departments/agencies or their agents?

10. Are there any known foreign business or government offices in adjacent buildings?

11. Provide the make and model number of all equipment used to process, transfer, or store classified information. Include computers, peripherals, network servers, network hardware, multiplexers, modems, encryption devices (COMSEC), etc.
12. Have on-site TEMPEST tests been conducted on any of this equipment? If so, which ones? When was the test(s) conducted? Who conducted the test(s)? Have all deficiencies (if any) been resolved?
13. Has a TEMPEST Facility Zoning test been conducted? If so, who conducted the testing and when?

## 8-7 DISSEMINATION OF TECHNICAL DOCUMENTS

1. DoD Directive 5230.24, Distribution Statements on Technical Documents, requires the assignment of distribution statements to facilitate control, distribution, and release of documents without the need to repeatedly refer questions to the originating command. The originating command may choose to make case-by-case exceptions to distribution limitations imposed by the statement. Distribution statements also provide the extent of secondary distribution that is permissible without further authorization or approval of the originating command.
2. All newly generated DoD unclassified technical documents shall bear one of the distribution statements described in Exhibit 8A. If not already in the public domain and likely to be disseminated outside the DOD, existing unclassified technical documents, including informal documents such as working papers, memoranda and preliminary reports shall be assigned a distribution statement from Exhibit 8A. Existing technical documents do not have to be reviewed for the sole purpose of assigning distribution statements but, when they are removed from files, a determination shall be made whether distribution limitations are necessary and, if so, they must be marked accordingly.
3. Classified technical documents shall be assigned Distribution Statements B, C, D, E, or F from Exhibit 8A. The distribution statement assigned to a classified document shall be retained on the document after its declassification or until specifically changed or removed by the originating command. Technical documents that are declassified and have no distribution statement assigned shall be handled per Distribution Statement F until changed by the originating command.
4. Information relating to NNPI which is not marked and handled as unclassified NNPI shall be reviewed and approved by the Naval Sea Systems Command (SEA-08) prior to release to the public.
5. This policy covers all newly created technical documents generated by all DoD-funded RDT&E programs which are the basis of the Navy Scientific and Technical Information Program described in reference (q) [SECNAVINST 3900.43A, Navy Scientific and Technical Information Program]. It applies to newly created engineering drawings, standards, specifications, technical manuals, blueprints, drawings, plans, instructions, computer software and documentation, and other technical information that can be used or be adapted for use to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment.
6. Reference (r) [OPNAVINST 5510.161, Withholding of Unclassified Technical Data from Public Disclosure] applies to unclassified technical data which reveals critical technology with military or space application and requires an approval, authorization, or license for its lawful export and which may be withheld from public disclosure (officially released under proper authority). This withholding authority does not apply to scientific, educational, or other data not directly and significantly related to design, production, or utilization in industrial processes.

## 8-8 PREPUBLICATION REVIEW

Reference (s) [SECNAVINST 5720.44A, DON Public Affairs Regulations] applies to public affairs and reference (t) [DoD Instruction 5230.39, Security and Policy Review of DoD Information for Public Release] applies to the clearance of DoD information for public release. Reference (u) [DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release] establishes the policy that a security and policy review shall be performed on all official DoD information intended for public release including information intended for placement on electronic bulletin boards accessible through the INTERNET or publicly accessible computer servers.

## Guide for Using Distribution Statements

### DISTRIBUTION STATEMENTS

REASONS FOR DESIGNATING A SPECIFIC STATEMENT	DISTRIBUTION STATEMENT						
	A	B	C	D	E	F	X
Approved for Public Release	Yes	No	No	No	No	No	No
Foreign Government Information	No	Yes	Yes	Yes	Yes	Yes	No
Proprietary Information	No	Yes	No	No	Yes	Yes	No
<b>Test and Evaluation</b>	<b>No</b>	<b>Yes</b>	<b>No</b>	<b>No</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>
Contractor Performance Evaluation	No	Yes	No	No	Yes	Yes	No
<b>Critical Technology</b>	<b>No</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>
Premature Dissemination	No	Yes	No	No	Yes	Yes	No
<b>Software Documentation</b>	<b>No</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>
<b>Administrative or Operational Use</b>	<b>No</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>	<b>No</b>
Specific Authority	No	Yes	Yes	Yes	Yes	Yes	Yes
Direct Military Support	No	No	No	No	Yes	Yes	No

**EXHIBIT 8A**

**PROCEDURES FOR ASSIGNING DISTRIBUTION  
STATEMENTS ON TECHNICAL DOCUMENTS**

1. **Newly generated unclassified technical documents** shall be assigned Distribution Statements A, B, C, D, E, F, or X. If not already in the public domain and are likely to be disseminated outside the DoD, existing unclassified technical documents shall be assigned Distribution Statements A, B, C, D, E, F, or X.
2. Technical documents in preliminary or working draft form shall not be disseminated without a proper security classification review and assignment of a distribution statement.
3. **Classified technical documents** shall be assigned Distribution Statements B, C, D, E, or F. The distribution statement assigned to a classified document shall be retained on the document after declassification or until specifically changed or removed by the originating command. If a technical document without a distribution statement is declassified, it shall be handled as a Distribution Statement F document until otherwise notified by the originating command.
4. If a newly generated technical document contains export-controlled technical data, it shall be marked with the statement in paragraph 1 under "ADDITIONAL NOTICES," in addition to Distribution Statements B, C, D, E, F, or X.
5. Scientific and technical documents which include a contractor-imposed "limited rights" statement shall be appropriately marked and controlled (see "CONTRACTOR-IMPOSED DISTRIBUTION LIMITATIONS" below).
6. The distribution statement shall be displayed conspicuously so it is readily recognized by recipients. For standard written or printed material, the distribution statement shall appear on the face of the document, title page, and DD 1473, "Report Documentation Page." When possible, parts that contain information creating the requirement for the distribution statement shall be prepared as an appendix to permit broader distribution of the basic document. When practicable, the abstract of the document, the DD 1473, and bibliographic citations shall be written in such a way that the information shall not be subject to Distribution Statements B, C, D, E, F, or X. If the technical information is not in standard written or printed form and does not have a cover or title page, the distribution statement shall be conspicuously stamped, printed, or written by other means.
7. Distribution statements remain in effect until changed or removed by the originating command. Each command shall establish and maintain a procedure for review of technical documents for which it is responsible, with the objective of increasing their availability as soon as conditions permit. Public release determinations shall be processed per DoD Instruction 5230.29 of 6 May 1996 (NOTAL). When public release clearance is obtained, Distribution Statement A shall be assigned and document handling facilities, including the Defense Technical Information Center (DTIC), shall be notified.

8. Technical documents with superseded distribution limitation markings shall be reviewed and assigned the appropriate distribution statement when a request for the document is received. Superseded distribution limitation markings shall be converted as follows:

- a. Documents with distribution marking A or B need not be reevaluated or remarked.
- b. Documents with distribution marking #2 shall be assigned Distribution Statement C.
- c. Documents with distribution marking #3 (U.S. Government Only) shall be assigned Distribution Statement B.
- d. Documents with distribution marking #4 (DoD Only) shall be assigned Distribution Statement E.
- e. Documents with distribution marking #5 (Controlled) shall be assigned Distribution Statement F.

9. Originating commands shall promptly notify DTIC and other information repositories holding their technical documents when:

- a. The address of designated originating commands is changed.
- b. The originating command is redesignated.
- c. Classification markings, distribution statements, or export control statements are changed.

## DISTRIBUTION STATEMENTS

1. The following distribution statements are authorized for use on technical documents:

a. "**DISTRIBUTION STATEMENT A:** Approved for public release; distribution is unlimited."

(1) This statement shall be used only on unclassified technical documents that have been cleared for public release by competent authority per DoD Instruction 5230.29 (NOTAL) and DoD Directive 5230.9 of 9 April 1996 (NOTAL).

(2) Technical documents resulting from contracted fundamental research efforts shall normally be assigned Distribution Statement A, except for those rare and exceptional circumstances where there is a high likelihood of disclosing performance characteristics of military systems, or of manufacturing technologies that are unique and critical to defense, and agreement on this situation has been recorded-in the contract or grant.

(3) Technical documents with this statement may be made available or sold to the public including foreign nationals, companies, and governments, and may be exported.

(4) This statement shall never be used on technical documents that formerly were classified without a positive determination of such releasability by the command exercising cognizance over the information prior to release.

(5) This statement shall not be used on classified technical documents or documents containing export-controlled technical data as provided in OPNAVINST 5510.161 of 29 July 1985.

b. "**DISTRIBUTION STATEMENT B:** Distribution authorized to U.S. Government agencies only; (fill in reason) (date). Other requests for this document shall be referred to (insert originating command)."

(1) This statement shall be used on unclassified or classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

(2) Reasons for assigning Distribution Statement B include:

(a) **FGI** - To protect and limit information distribution per the desires of the foreign government that furnished the technical information. Information of this type is normally classified at the Confidential level or higher.

(b) **Proprietary Information** - To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it may not be routinely transmitted outside the U.S. Government.

(c) **Critical Technology** - To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled and subject to the provisions of OPNAVINST 5510.161 of 29 July 1985.

(d) **Test and Evaluation** - To protect results of test and evaluation of commercial products or military hardware when disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

(e) **Contractor Performance Evaluation** - To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

(f) **Premature Dissemination** - To protect patentable information on systems or processes in the developmental or concept stage from premature dissemination.

(g) **Administrative/Operational Use** - To protect technical or operational information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement shall be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

(h) **Software Documentation** - Releasable only per the provisions of DoD instruction 7930.2 of 31 December 1979 (NOTAL).

(i) **Specific Authority** - To protect information not specifically included in the above reasons and discussions, but which requires protection per valid documented authority such as E.O.s, classification guidelines, DoD or DON regulations, or policy guidance. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

c. "**DISTRIBUTION STATEMENT C:** Distribution authorized to U.S. Government agencies and their contractors; (fill in reason) (date). Other requests for this document shall be referred to (insert originating command)."

(1) May be used on unclassified or classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

(2) Reasons for assigning Distribution Statement C include:

(a) FGI - Same as Distribution Statement B.

(b) Critical Technology - Same as Distribution Statement B.

(c) Software Documentation - Same as Distribution Statement B.

(d) Administrative or Operational Use - Same as Distribution Statement B.

(e) Specific Authority - Same as Distribution Statement B.

d. "**DISTRIBUTION STATEMENT D:** Distribution authorized to DoD and DoD contractors only; (fill in reason) (date). Other U.S. requests shall be referred to (insert originating command)."

(1) May be used on unclassified or classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

(2) Reasons for assigning Distribution Statement D include:

(a) FGI - Same as Distribution Statement B.

(b) Administrative or operational Use - Same as Distribution Statement B.

(c) Software Documentation - Same as Distribution Statement B.

(d) Critical Technology - Same as Distribution Statement B.

(e) Specific Authority - Same as Distribution Statement B.

e. "**DISTRIBUTION STATEMENT E:** Distribution authorized to DOD Components Only; (fill in reason) (date). Other requests shall be referred to (insert originating command)."

(1) May be used on unclassified or classified technical documents if necessary to ensure distribution limitation in addition to need-to-know requirements of this regulation or in the event the document is declassified.

(2) Reasons for assigning Distribution Statement E include:

(a) Direct Military Support - Document contains export-controlled technical data of such military significance that release for purposes other than direct support of DoD approved activities may jeopardize an important technological or operational military advantage of the U.S. Designation of such data is made by competent authority per OPNAVINST 5510.161 of 29 July 1985.

(b) FGI - Same as Distribution Statement B.

(c) Proprietary Information - Same as Distribution Statement B.

(d) Premature Dissemination - Same as Distribution Statement B.

(e) Test and Evaluation - Same as Distribution Statement B.

- (f) Software Documentation - Same as Distribution Statement B.
- (g) Contractor Performance and Evaluation - Same as Distribution Statement B.
- (h) Critical Technology - Same as Distribution Statement B.
- (i) Administrative/operational Use - Same as Distribution Statement B.
- (j) Specific Authority - Same as Distribution Statement B.

f. **"DISTRIBUTION STATEMENT F:** Further dissemination only as directed by (insert originating command) (date) or higher DOD authority."

(1) Normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists.

(2) Distribution Statement F is used when the originator determines that the information is subject to the special dissemination limitation specified in chapter 6, paragraph 6-11.3a.

(3) When a classified document assigned Distribution Statement F is declassified, the statement shall be retained until specifically changed or removed by the originating command.

g. **"DISTRIBUTION STATEMENT X:** Distribution authorized to U.S. Government agencies and private individuals or enterprises eligible to obtain export-controlled technical data in accordance with OPNAVINST 5510.161. Other requests shall be referred to (originating command)."

(1) This statement shall be used on unclassified documents when Distribution Statements B, C, D, E, or F are not applicable but the document contains technical data per OPNAVINST 5510.161 of 29 July 1985.

(2) This statement shall not be used on classified technical documents. It may be assigned to technical documents that formerly were classified.

#### ADDITIONAL NOTICES

1. In addition to the distribution statement, the following notices shall be used when appropriate:
  - a. All technical documents determined to contain export controlled technical data shall be marked **"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 per the provisions of OPNAVINST 5510.161."** When it is technically impracticable to use the entire statement, an abbreviated marking shall be used, and a copy of the full statement added to the "Notice To Accompany Release of Export Controlled Data," required by OPNAVINST 5510.161 of 29 July 1985.
2. Unclassified/Limited Distribution documents shall be handled using the same standard as FOUO information, and shall be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicate that this destruction method is not sufficiently protective of unclassified limited information, local authorities may prescribe other methods but must give due consideration to the additional expense balanced against the degree of sensitivity.

#### CONTRACTOR IMPOSED DISTRIBUTION LIMITATIONS

1. Contractors may have proprietary technical data to which the U.S. Government is given limited rights. The contractor shall place a limited rights statement on each document containing contractor controlled technical data furnished to the U.S. Government. Documents with limited rights information shall be assigned Distribution Statements B, E, or F.
2. Limited rights is defined as the right to use, duplicate, or disclose technical data in whole or in part, by or for the U.S. Government, with the express limitation that such technical data, without the written permission of the party furnishing the technical data, shall not be:
  - a. Released or disclosed in whole or in part outside the U.S. Government.
  - b. Used in whole or in part by the U.S. Government for manufacture, or in the case of computer software documentation, for reproduction of the computer software.
  - c. Used by a party other than the U.S. Government, except for:
    - (1) Emergency repair or overhaul work only by or for the U.S. Government, when the item or process concerned is not otherwise reasonably available to enable timely performance of the work, provided that the release or disclosure outside the U.S. Government will be made subject to a prohibition against further use, release, or disclosure; or

SECNAVINST 5510.36  
17 MAR 1999

(2) Release to a foreign government, as the interest of the U.S. Government may require, only for information or evaluation within the foreign government or for emergency repair or overhaul work by or for the foreign government under the conditions of subparagraph (1) above.

3. The limited rights statement remains in effect until changed or cancelled under contract terms or with the permission of the contractor and the controlling office notifies recipients of the document that the statement has been changed or cancelled. Upon cancellation of the limited rights statement, the distribution, disclosure, or release of the technical document will then be controlled by its security classification or, if it is unclassified, by the appropriate distribution statement.

EXHIBIT 8B

**CATEGORIES OF INFORMATION WHICH REQUIRE REVIEW AND CLEARANCE  
BY THE ASD(PA) PRIOR TO PUBLIC RELEASE**

1. Certain categories of information require review and clearance by the ASD(PA) via the CNO (N09N2) before public release. They include information which:

- a. Originates or is proposed for public release in the Washington, D.C. area;
- b. Is or has the potential to become an item of national or international interest;
- c. Affects national security policy or foreign relations;
- d. Concerns a subject of potential controversy among the DOD components or with other federal agencies;
- e. Is presented by a DOD employee, who by virtue of rank, position, or expertise would be considered an official DOD spokes person;
- f. Contains technical data, including data developed under contract or independently developed and controlled by the International Traffic in Arms Regulation (ITAR), that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made; or,
- g. Bears on any of the following subjects:
  - (1) New weapons or weapons systems, significant modifications or improvements to existing weapons, weapons systems, equipment, or techniques.
  - (2) Military operations, significant exercises, and operations security.
  - (3) National Command Authorities; command, control, communications, computers, and intelligence; information warfare; and computer security.
  - (4) Military activities or application in space; nuclear weapons, including nuclear weapons effects research; chemical warfare and defensive biological warfare; and arms control treaty implementation.

### C3. CHAPTER 3

#### EXEMPTIONS

##### C3.1. GENERAL PROVISIONS

C3.1.1. General. Records that meet the exemption criteria of the FOIA may be withheld from public disclosure and need not be published in the Federal Register, made available in a library reading room, or provided in response to a FOIA request.

##### C3.2. EXEMPTIONS

C3.2.1. FOIA Exemptions. The following types of records may be withheld in whole or in part from public disclosure under the FOIA, unless otherwise prescribed by law: A discretionary release of a record (see also subsection C1.5.5., above) to one requester shall prevent the withholding of the same record under a FOIA exemption if the record is subsequently requested by someone else. However, a FOIA exemption may be invoked to withhold information that is similar or related that has been the subject of a discretionary release. In applying exemptions, the identity of the requester and the purpose for which the record is sought are irrelevant with the exception that an exemption may not be invoked where the particular interest to be protected is the requester's interest. *However, if the subject of the record is the requester for the record and the record is contained in a Privacy Act system of records, it may only be denied to the requester if withholding is both authorized by DoD 5400.11-R (reference (v)) and by a FOIA exemption.*

C3.2.1.1. Number 1. (5 U.S.C. 552 (b)(1)) (reference (a)). Those properly and currently classified in the interest of national defense or foreign policy, as specifically authorized under the criteria established by Executive Order and implemented by regulations, such as DoD 5200.1-R (reference (g)). Although material is not classified at the time of the FOIA request, a classification review may be undertaken to determine whether the information should be classified. The procedures in reference (g) apply. If the information qualifies as Exemption 1 information, there is **no discretion** regarding its release. In addition, this exemption shall be invoked when the following situations are apparent:

C3.2.1.1.1. The fact of the existence or nonexistence of a record would itself reveal classified information. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. A

"refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no record" response when a record does not exist, and a "refusal to confirm or deny" when a record does exist will itself disclose national security information.

C3.2.1.1.2. Compilations of items of information that are individually unclassified may be classified if the compiled information reveals additional association or relationship that meets the standard for classification under an existing executive order for classification and DoD 5200.1-R (reference (g)), and is not otherwise revealed in the individual items of information.

C3.2.1.2. Number 2. (5 U.S.C. 552 (b)(2)) (reference (a)). Those related solely to the internal personnel rules and practices of the Department of Defense or any of its Components. This exemption is **entirely discretionary**. This exemption has two profiles, **high (b)(2) and low (b)(2)**. Paragraph C3.2.1.2.2., below, contains a brief discussion on the low (b)(2) profile; however, that discussion is for information purposes only. When only a minimum Government interest would be affected (administrative burden), there is a great potential for discretionary disclosure of the information. Consequently, DoD Components **shall not invoke** the low (b)(2) profile.

C3.2.1.2.1. Records qualifying under high (b)(2) are those containing or constituting statutes, rules, regulations, orders, manuals, directives, instructions, and security classification guides, the release of which would allow circumvention of these records thereby substantially hindering the effective performance of a significant function of the Department of Defense. Examples include:

C3.2.1.2.1.1. Those operating rules, guidelines, and manuals for DoD investigators, inspectors, auditors, or examiners that must remain privileged in order for the DoD Component to fulfill a legal requirement.

C3.2.1.2.1.2. Personnel and other administrative matters, such as examination questions and answers used in training courses or in the determination of the qualifications of candidates for employment, entrance on duty, advancement, or promotion.

C3.2.1.2.1.3. Computer software, the release of which would allow circumvention of a statute or DoD rules, Regulations, orders, Manuals, Directives, or Instructions. In this situation, the use of the software must be closely examined to ensure a circumvention possibility exists.

C3.2.1.2.2. Records qualifying under the low (b)(2) profile are those that are trivial and housekeeping in nature for which there is no legitimate public interest or benefit to be gained by release, and it would constitute an administrative burden to process the request in order to disclose the records. Examples include rules of personnel's use of parking facilities or regulation of lunch hours, statements of policy as to sick leave, and administrative data such as file numbers, mail routing stamps, initials, data processing notations, brief references to previous communications, and other like administrative markings. DoD Components shall not invoke the low (b)(2) profile.

C3.2.1.3. Number 3. (5 U.S.C. 552 (b)(3)) (reference (a)). Those concerning matters that a statute specifically exempts from disclosure by terms that permit **no discretion** on the issue, or in accordance with criteria established by that statute for withholding or referring to particular types of matters to be withheld. The Directorate for Freedom of Information and Security Review maintains a list of (b)(3) statutes used within the Department of Defense, and provides updated lists of these statutes to DoD Components on a periodic basis. A few examples of such statutes are:

C3.2.1.3.1. Patent Secrecy, 35 U.S.C. 181-188 (reference (h)). Any records containing information relating to inventions that are the subject of patent applications on which Patent Secrecy Orders have been issued.

C3.2.1.3.2. Restricted Data and Formerly Restricted Data, 42 U.S.C. 2162 (reference (i)).

C3.2.1.3.3. Communication Intelligence, 18 U.S.C. 798 (reference (j)).

C3.2.1.3.4. Authority to Withhold From Public Disclosure Certain Technical Data, 10 U.S.C. 130 and DoD Directive 5230.25 (references (k) and (l)).

C3.2.1.3.5. Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants, 10 U.S.C. 1102 f (reference (m)).

C3.2.1.3.6. Physical Protection of Special Nuclear Material: Limitation on Dissemination of Unclassified Information, 10 U.S.C. 128 (reference (n)).

C3.2.1.3.7. Protection of Intelligence Sources and Methods, 50 U.S.C. 403-3(c)(6) (reference (o)).

C3.2.1.3.8. Protection of Contractor Submitted Proposals, 10 U.S.C.

2305(g) (reference (p)).

C3.2.1.3.9. Procurement Integrity, 41 U.S.C. 423 (reference (q)).

C3.2.1.4. Number 4. (5 U.S.C. 552 (b)(4)) (reference (a)). Those containing trade secrets or commercial or financial information that a DoD Component receives from a person or organization outside the Government with the understanding that the information or record will be retained on a privileged or confidential basis in accordance with the customary handling of such records. Records within the exemption must contain trade secrets, or commercial or financial records, the disclosure of which is likely to cause substantial harm to the competitive position of the source providing the information; impair the Government's ability to obtain necessary information in the future; or impair some other legitimate Government interest. Commercial or financial information submitted on a voluntary basis, absent any exercised authority prescribing criteria for submission is protected without any requirement to show competitive harm (see paragraph C3.2.1.4.8., below). If the information qualifies as Exemption 4 information, there is **no discretion** in its release. Examples include:

C3.2.1.4.1. Commercial or financial information received in confidence in connection with loans, bids, contracts, or proposals set forth in or incorporated by reference in a contract entered into between the DoD Component and the offeror that submitted the proposal, as well as other information received in confidence or privileged, such as trade secrets, inventions, discoveries, or other proprietary data. See also C5.2.8.2., below, this Regulation. Additionally, when the provisions of 10 U.S.C. 2305(g) (reference (p)), and 41 U.S.C. 423 (reference (q)) are met, certain proprietary and source selection information may be withheld under Exemption 3.

C3.2.1.4.2. Statistical data and commercial or financial information concerning contract performance, income, profits, losses, and expenditures, if offered and received in confidence from a contractor or potential contractor.

C3.2.1.4.3. Personal statements given in the course of inspections, investigations, or audits, when such statements are received in confidence from the individual and retained in confidence because they reveal trade secrets or commercial or financial information normally considered confidential or privileged.

C3.2.1.4.4. Financial data provided in confidence by private employers in connection with locality wage surveys that are used to fix and adjust pay schedules applicable to the prevailing wage rate of employees within the Department of Defense.

C3.2.1.4.5. Scientific and manufacturing processes or developments concerning technical or scientific data or other information submitted with an application for a research grant, or with a report while research is in progress.

C3.2.1.4.6. Technical or scientific data developed by a contractor or subcontractor exclusively at private expense, and technical or scientific data developed in part with Federal funds and in part at private expense, wherein the contractor or subcontractor has retained legitimate proprietary interests in such data in accordance with 10 U.S.C. 2320-2321 (reference (r)) and DoD Federal Acquisition Regulation Supplement (DFARS), Chapter 2 of 48 C.F.R., Subpart 227.71-227.72 (reference (s)). Technical data developed exclusively with Federal funds may be withheld under Exemption Number 3 if it meets the criteria of 10 U.S.C. 130 (reference (k)) and DoD Directive 5230.25 (reference (l)) (see subsection C3.2.1., Number 3 C3.2.1.3.5., above).

C3.2.1.4.7. Computer software which is copyrighted under the Copyright Act of 1976 (17 U.S.C. 106) (reference (t)), the disclosure of which would have an adverse impact on the potential market value of a copyrighted work.

C3.2.1.4.8. Proprietary information submitted strictly on a **voluntary** basis, absent any exercised authority prescribing criteria for submission. Examples of exercised authorities prescribing criteria for submission are statutes, Executive Orders, regulations, invitations for bids, requests for proposals, and contracts. Submission of information under these authorities is **not voluntary**. (See also subsection C5.2.8.3., below.)

C3.2.1.5. Number 5. (5 U.S.C. 552 (b)(5)) (reference (a)). Those containing information considered privileged in litigation, primarily under the deliberative process privilege. Except as provided in paragraphs Number 5 C3.2.1.5.2. through C3.2.1.5.5., below, internal advice, recommendations, and subjective evaluations, as contrasted with factual matters, that are reflected in deliberative records pertaining to the decision-making process of an Agency, whether within or among Agencies (as defined in 5 U.S.C. 552(e) (reference (a))), or within or among DoD Components. In order to meet the test of this exemption, the record must be both deliberative in nature, as well as part of a decision-making process. Merely being an internal record is insufficient basis for withholding under this exemption. Also potentially exempted are records pertaining to the attorney-client privilege and the attorney work-product privilege. This exemption is **entirely discretionary**.

C3.2.1.5.1. Examples of the deliberative process include:

C3.2.1.5.1.1. The non-factual portions of staff papers, to include after-action reports, lessons learned, and situation reports containing staff evaluations, advice, opinions, or suggestions.

C3.2.1.5.1.2. Advice, suggestions, or evaluations prepared on behalf of the Department of Defense by individual consultants or by boards, committees, councils, groups, panels, conferences, commissions, task forces, or other similar groups that are formed for the purpose of obtaining advice and recommendations.

C3.2.1.5.1.3. Those non-factual portions of evaluations by DoD Component personnel of contractors and their products.

C3.2.1.5.1.4. Information of a speculative, tentative, or evaluative nature or such matters as proposed plans to procure, lease or otherwise acquire and dispose of materials, real estate, facilities or functions, when such information would provide undue or unfair competitive advantage to private personal interests or would impede legitimate Government functions.

C3.2.1.5.1.5. Trade secret or other confidential research development, or commercial information owned by the Government, where premature release is likely to affect the Government's negotiating position or other commercial interest.

C3.2.1.5.1.6. Those portions of official reports of inspection, reports of the Inspector Generals, audits, investigations, or surveys pertaining to safety, security, or the internal management, administration, or operation of one or more DoD Components, when these records have traditionally been treated by the courts as privileged against disclosure in litigation.

C3.2.1.5.1.7. Planning, programming, and budgetary information that is involved in the defense planning and resource allocation process.

C3.2.1.5.2. If any such intra- or inter-agency record or reasonably segregable portion of such record hypothetically would be made available routinely through the discovery process in the course of litigation with the Agency, then it should not be withheld under the FOIA. If, however, the information hypothetically would not be released at all, or would only be released in a particular case during civil

discovery where a party's particularized showing of need might override a privilege, then the record may be withheld. Discovery is the formal process by which litigants obtain information from each other for use in the litigation. Consult with legal counsel to determine whether Exemption 5 material would be routinely made available through the discovery process.

C3.2.1.5.3. Intra- or inter-agency memoranda or letters that are factual, or those reasonably segregable portions that are factual, are routinely made available through discovery, and shall be made available to a requester, unless the factual material is otherwise exempt from release, inextricably intertwined with the exempt information, so fragmented as to be uninformative, or so redundant of information already available to the requester as to provide no new substantive information.

C3.2.1.5.4. A direction or order from a superior to a subordinate, though contained in an internal communication, generally cannot be withheld from a requester if it constitutes policy guidance or a decision, as distinguished from a discussion of preliminary matters or a request for information or advice that would compromise the decision-making process.

C3.2.1.5.5. An internal communication concerning a decision that subsequently has been made a matter of public record must be made available to a requester when the rationale for the decision is expressly adopted or incorporated by reference in the record containing the decision.

C3.2.1.6. Number 6. (5 U.S.C. 552 (b)(6)) (reference (a)). Information in personnel and medical files, as well as similar personal information in other files, that, if disclosed to a requester, other than the person about whom the information is about, would result in a clearly unwarranted invasion of personal privacy. Release of information about an individual contained in a Privacy Act System of records that would constitute a clearly unwarranted invasion of privacy is prohibited, and could subject the releaser to civil and criminal penalties. If the information qualifies as Exemption 6 information, there is **no discretion** in its release.

C3.2.1.6.1. Examples of other files containing personal information similar to that contained in personnel and medical files include:

C3.2.1.6.1.1. Those compiled to evaluate or adjudicate the suitability of candidates for civilian employment or membership in the Armed Forces, and the eligibility of individuals (civilian, military, or contractor employees) for security clearances, or for access to particularly sensitive classified information.

C3.2.1.6.1.2. Files containing reports, records, and other material pertaining to personnel matters in which administrative action, including disciplinary action, may be taken.

C3.2.1.6.2. Home addresses, *including private e-mail addresses*, are normally not releasable without the consent of the individuals concerned. This includes lists of home addressees and military quarters' addressees without the occupant's name. *Additionally, the names and duty addresses (postal and/or e-mail) of DoD military and civilian personnel who are assigned to units that are sensitive, routinely deployable, or stationed in foreign territories can constitute a clearly unwarranted invasion of personal privacy.*

C3.2.1.6.2.1. Privacy Interest. A privacy interest may exist in personal information even though the information has been disclosed at some place and time. If personal information is not freely available from sources other than the Federal Government, a privacy interest exists in its nondisclosure. The fact that the Federal Government expended funds to prepare, index and maintain records on personal information, and the fact that a requester invokes FOIA to obtain these records indicates the information is not freely available.

C3.2.1.6.2.2. Names and duty addresses (*postal and/or e-mail*) published in telephone directories, organizational charts, rosters and similar materials for personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories are withholdable under this exemption.

C3.2.1.6.3. This exemption shall not be used in an attempt to protect the privacy of a deceased person, but it may be used to protect the privacy of the deceased person's family if disclosure would rekindle grief, anguish, pain, embarrassment, or even disruption of peace of mind of surviving family members. In such situations, balance the surviving family members' privacy against the public's right to know to determine if disclosure is in the public interest. Additionally, the deceased's social security number should be withheld since it is used by the next of kin to receive benefits. Disclosures may be made to the immediate next of kin as defined in DoD Directive 5154.24 (reference (u)).

C3.2.1.6.4. A clearly unwarranted invasion of the privacy of third parties identified in a personnel, medical or similar record constitutes a basis for deleting those reasonably segregable portions of that record. When withholding third party personal information from the subject of the record and the record is contained in

a Privacy Act system of records, consult with legal counsel.

C3.2.1.6.5. This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, DoD Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption 6 must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

C3.2.1.6.5.1. A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

C3.2.1.6.5.2. Refusal to confirm or deny should not be used when (a) the person whose personal privacy is in jeopardy has provided the requester a waiver of his or her privacy rights; (b) the person initiated or directly participated in an investigation that lead to the creation of an Agency record seeks access to that record; or (c) the person whose personal privacy is in jeopardy is deceased, the Agency is aware of that fact, and disclosure would not invade the privacy of the deceased's family. See paragraph Number C3.2.1.6.3., above.

C3.2.1.7. Number 7. (5 U.S.C. 552 (b)(7)) (reference (a)). Records or information compiled for law enforcement purposes; i.e., civil, criminal, or military law, including the implementation of Executive Orders or regulations issued pursuant to law. This exemption may be invoked to prevent disclosure of documents not originally created for, but later gathered for law enforcement purposes. **With the exception of parts (C) and (F)** (see subparagraph Number 7 C3.2.1.7.1.3., below) of this exemption, this exemption is **discretionary**. If information qualifies as exemption **(7)(C) or (7)(F)** (see subparagraph Number 7 C3.2.1.7.1.3., below) information, there is **no discretion** in its release.

C3.2.1.7.1. This exemption applies, however, only to the extent that production of such law enforcement records or information could result in the following:

C3.2.1.7.1.1. Could reasonably be expected to interfere with enforcement proceedings (5 U.S.C. 552(b)(7)(A)) (reference (a)).

C3.2.1.7.1.2. Would deprive a person of the right to a fair trial or to an impartial adjudication (5 U.S.C. 552(b)(7)(B)) (reference (a)).

C3.2.1.7.1.3. Could reasonably be expected to constitute an unwarranted invasion of personal privacy of a living person, including surviving family members of an individual identified in such a record (5 U.S.C. 552(b)(7)(C)) (reference (a)).

C3.2.1.7.1.3.1. This exemption also applies when the fact of the existence or nonexistence of a responsive record would itself reveal personally private information, and the public interest in disclosure is not sufficient to outweigh the privacy interest. In this situation, Components shall neither confirm nor deny the existence or nonexistence of the record being requested. This is a Glomar response, and Exemption (7)(C) must be cited in the response. Additionally, in order to insure personal privacy is not violated during referrals, DoD Components shall coordinate with other DoD Components or Federal Agencies **before** referring a record that is exempt under the Glomar concept.

C3.2.1.7.1.3.2. A "refusal to confirm or deny" response must be used consistently, not only when a record exists, but also when a record does not exist. Otherwise, the pattern of using a "no records" response when a record does not exist and a "refusal to confirm or deny" when a record does exist will itself disclose personally private information.

C3.2.1.7.1.3.3. Refusal to confirm or deny should not be used when 1 the person whose personal privacy is in jeopardy has provided the requester with a waiver of his or her privacy rights; or 2 the person whose personal privacy is in jeopardy is deceased, and the Agency is aware of that fact.

C3.2.1.7.1.3.4. Could reasonably be expected to disclose the identity of a confidential source, including a source within the Department of Defense; a State, local, or foreign agency or authority; or any private institution that furnishes the information on a confidential basis; and could disclose information furnished from a confidential source and obtained by a criminal law enforcement authority in a criminal investigation or by an Agency conducting a lawful national security intelligence investigation (5 U.S.C. 552(b)(7)(D)) (reference (a)).

C3.2.1.7.1.3.5. Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law (5 U.S.C. 552(b)(7)(E)) (reference (a)).

C3.2.1.7.1.3.6. Could reasonably be expected to endanger the life or physical safety of any individual (5 U.S.C. 552(b)(7)(F)) (reference (a)).

C3.2.1.7.2. Some examples of Exemption 7 are:

C3.2.1.7.2.1. Statements of witnesses and other material developed during the course of the investigation and all materials prepared in connection with related Government litigation or adjudicative proceedings.

C3.2.1.7.2.2. The identity of firms or individuals being investigated for alleged irregularities involving contracting with the Department of Defense when no indictment has been obtained nor any civil action filed against them by the United States.

C3.2.1.7.2.3. Information obtained in confidence, expressed or implied, in the course of a criminal investigation by a criminal law enforcement Agency or office within a DoD Component, or a lawful national security intelligence investigation conducted by an authorized Agency or office within a DoD Component. National security intelligence investigations include background security investigations and those investigations conducted for the purpose of obtaining affirmative or counterintelligence information.

C3.2.1.7.3. The right of individual litigants to investigative records currently available by law (such as, the Jencks Act, 18 U.S.C. 3500, (reference (w))) is not diminished.

C3.2.1.7.4. Exclusions. Excluded from the above exemption are the below two situations applicable to the Department of Defense. (Components considering invoking an exclusion should first consult with the Department of Justice, Office of Information and Privacy.)

C3.2.1.7.4.1. Whenever a request is made that involves access to records or information compiled for law enforcement purposes, and the investigation or proceeding involves a possible violation of criminal law where there is reason to believe that the subject of the investigation or proceeding is unaware of its pendency,

and the disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, Components may, during only such times as that circumstance continues, treat the records or information as not subject to the FOIA. In such situation, the response to the requester will state that no records were found.

C3.2.1.7.4.2. Whenever informant records maintained by a criminal law enforcement organization within a DoD Component under the informant's name or personal identifier are requested by a third party using the informant's name or personal identifier, the Component may treat the records as not subject to the FOIA, unless the informant's status as an informant has been officially confirmed. If it is determined that the records are not subject to 5 U.S.C. 552(b)(7) (reference (a)), the response to the requester will state that no records were found.

C3.2.1.8. Number 8. (5 U.S.C. 552 (b)(8)) (reference (a)). Those contained in or related to examination, operation or condition reports prepared by, on behalf of, or for the use of any Agency responsible for the regulation or supervision of financial institutions.

C3.2.1.9. Number 9. (5 U.S.C. 552 (b)(9)) (reference (a)). Those containing geological and geophysical information and data (including maps) concerning wells.

C4. CHAPTER 4  
FOR OFFICIAL USE ONLY

C4.1. GENERAL PROVISIONS

C4.1.1. General. Information that has not been given a security classification pursuant to the criteria of an Executive Order, but which may be withheld from the public *because disclosure would cause a foreseeable harm to an interest protected by one or more FOIA Exemptions 2 through 9 (see Chapter C3\*)* shall be considered as being for official use only (FOUO). No other material shall be considered FOUO and FOUO is not authorized as an anemic form of classification to protect national security interests. Additional information on FOUO and other controlled, unclassified information may be found in reference (g) *or by contacting the Directorate for Security, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence)*.

C4.1.2. Prior FOUO Application. The prior application of FOUO markings is not a conclusive basis for withholding a record that is requested under the FOIA. When such a record is requested, the information in it shall be evaluated to determine whether *disclosure would result in a foreseeable harm to an interest protected by one or more FOIA Exemptions 2 through 9*. Even if any exemptions apply, the record shall be released as a discretionary matter when it is determined that *there is no foreseeable harm to an interest protected by the exemptions*.

C4.1.3. Historical Papers. Records such as notes, working papers, and drafts retained as historical evidence of DoD Component actions enjoy no special status apart from the exemptions under the FOIA (reference (a)).

C4.1.4. Time to Mark Records. The marking of records at the time of their creation provides notice of FOUO content and facilitates review when a record is requested under the FOIA. Records requested under the FOIA that do not bear such markings shall not be assumed to be releasable without examination for the presence of information that requires continued protection and qualifies as exempt from public release.

C4.1.5. Distribution Statement. Information in a technical document that requires a distribution statement pursuant to DoD Directive 5230.24 (reference (x)) shall bear that statement and may be marked FOUO, as appropriate.

## C4.2. MARKINGS

### C4.2.1. Location of Markings.

C4.2.1.1. An unclassified document containing FOUO information shall be marked "For Official Use Only" at the bottom on the outside of the front cover (if any), on each page containing FOUO information, and on the outside of the back cover (if any). *Each paragraph containing FOUO information shall be marked as such.*

C4.2.1.2. Within a classified document, an individual page that contains both FOUO and classified information shall be marked at the top and bottom with the highest security classification of information appearing on the page. Individual paragraphs shall be marked at the appropriate classification level, as well as unclassified or FOUO, as appropriate.

C4.2.1.3. Within a classified document, an individual page that contains FOUO information but no classified information shall be marked "For Official Use Only" at the top and bottom of the page, *as well as each paragraph that contains FOUO information.*

C4.2.1.4. Other records, such as photographs, films, tapes, or slides, shall be marked "For Official Use Only" or "FOUO" in a manner that ensures that a recipient or viewer is aware of the status of the information therein.

C4.2.1.5. FOUO material transmitted outside the Department of Defense requires application of an expanded marking to explain the significance of the FOUO marking. This may be accomplished by typing or stamping the following statement on the record prior to transfer:

This document contains information  
EXEMPT FROM MANDATORY DISCLOSURE  
under the FOIA. Exemption(s) . . . . . applies/apply.

## C4.3. DISSEMINATION AND TRANSMISSION

C4.3.1. Release and Transmission Procedures. Until FOUO status is terminated, the release and transmission instructions that follow apply:

C4.3.1.1. FOUO information may be disseminated within DoD Components and between officials of DoD Components and DoD contractors, consultants, and grantees to conduct official business for the Department of Defense. Recipients shall be made aware of the status of such information, and transmission shall be by means that preclude unauthorized public disclosure. Transmittal documents shall call attention to the presence of FOUO attachments.

C4.3.1.2. DoD holders of FOUO information are authorized to convey such information to officials in other Departments and Agencies of the Executive and Judicial Branches to fulfill a Government function, except to the extent prohibited by the Privacy Act. Records thus transmitted shall be marked "For Official Use Only," and the recipient shall be advised that the information may qualify for exemption from public disclosure, pursuant to the FOIA, and that special handling instructions do or do not apply.

C4.3.1.3. Release of FOUO information to Members of Congress is governed by DoD Directive 5400.4 (reference (y)). Release to the GAO is governed by DoD Directive 7650.1 (reference (z)). Records released to the Congress or GAO should be reviewed to determine whether the information warrants FOUO status. If not, prior FOUO markings shall be removed or effaced. If withholding criteria are met, the records shall be marked FOUO and the recipient provided an explanation for such exemption and marking. Alternatively, the recipient may be requested, without marking the record, to protect against its public disclosure for reasons that are explained.

C4.3.2. Transporting FOUO Information. Records containing FOUO information shall be transported in a manner that prevents disclosure of the contents. When not commingled with classified information, FOUO information may be sent via first-class mail or parcel post. Bulky shipments, such as distributions of FOUO Directives or testing materials, that otherwise qualify under postal regulations, may be sent by fourth-class mail.

C4.3.3. Electronically and Facsimile Transmitted Messages. Each part of electronically and facsimile transmitted messages containing FOUO information shall be marked appropriately. Unclassified messages containing FOUO information shall contain the abbreviation "FOUO" before the beginning of the text. Such messages and facsimiles shall be transmitted in accordance with communications security procedures whenever practicable.

#### C4.4. SAFEGUARDING FOUO INFORMATION

C4.4.1. During Duty Hours. During normal working hours, records determined to be FOUO shall be placed in an out-of-sight location if the work area is accessible to non-government personnel.

C4.4.2. During Nonduty Hours. At the close of business, FOUO records shall be stored so as to prevent unauthorized access. Filing such material with other unclassified records in unlocked files or desks, etc., is adequate when normal U.S. Government or Government-contractor internal building security is provided during nonduty hours. When such internal security control is not exercised, locked buildings or rooms normally provide adequate after-hours protection. If such protection is not considered adequate, FOUO material shall be stored in locked receptacles such as file cabinets, desks, or bookcases. FOUO records that are subject to the provisions of the National Security Act of 1959 (reference (aa)) shall meet the safeguards outlined for that group of records.

#### C4.5. TERMINATION, DISPOSAL AND UNAUTHORIZED DISCLOSURES

C4.5.1. Termination. The originator or other competent authority; e.g., initial denial and appellate authorities, shall terminate "For Official Use Only" markings or status when circumstances indicate that the information no longer requires protection from public disclosure. When FOUO status is terminated, all known holders shall be notified, to the extent practical. Upon notification, holders shall efface or remove the "For Official Use Only" markings, but records in file or storage need not be retrieved solely for that purpose.

##### C4.5.2. Disposal.

C4.5.2.1. Nonrecord copies of FOUO materials may be destroyed by tearing each copy into pieces to prevent reconstructing, and placing them in regular trash containers. When local circumstances or experience indicates that this destruction method is not sufficiently protective of FOUO information, local authorities may direct other methods but must give due consideration to the additional expense balanced against the degree of sensitivity of the type of FOUO information contained in the records.

C4.5.2.2. Record copies of FOUO documents shall be disposed of in

accordance with the disposal standards established under 44 U.S.C. 3301-3314 (reference (ab)), as implemented by DoD Component instructions concerning records disposal.

C4.5.3. Unauthorized Disclosure. The unauthorized disclosure of FOUO records does not constitute an unauthorized disclosure of DoD information classified for security purposes. Appropriate administrative action shall be taken, however, to fix responsibility for unauthorized disclosure whenever feasible, and appropriate disciplinary action shall be taken against those responsible. Unauthorized disclosure of FOUO information that is protected by the Privacy Act (reference (d)) may also result in civil and criminal sanctions against responsible persons. The DoD Component that originated the FOUO information shall be informed of its unauthorized disclosure.

**INSTRUCTIONS FOR COMPLETING DD FORM 1540,  
"REGISTRATION FOR SCIENTIFIC AND TECHNICAL INFORMATION SERVICES"**

**A. WHO IS ELIGIBLE**

The Defense Technical Information Center's (DTIC's) products and services are available to U.S. Government organizations, their contractors, subcontractors and potential contractors. In order to register for these services, all applicants are required to complete the DD Form 1540.

**B. WHERE TO FILE**

Completed DD Forms 1540, and other related correspondence, should be mailed to:

Defense Technical Information Center  
DTIC-BCS, Registration Branch  
8725 John J. Kingman Road  
Suite 0944  
Fort Belvoir, VA 22060-6218

Telephone: (703) 767-8273  
Fax: (703) 767-8228

**C. RESTRICTED DATA AND/OR CNWDI**

U.S. Government (Non-DoD) organizations requesting access to Restricted Data and/or CNWDI must have the Department of Energy notify DTIC in writing that the individual listed as the point-of-contact (Item 4, "Attention") on the DD Form 1540 is authorized to receive such data.

**D. GENERAL INSTRUCTIONS**

**1. U.S. Government Organizations**

(1) Section I - General Information. All applicants must complete Section I in full.

- DoD organizations complete only Section I if requesting access to unclassified/unlimited or unclassified/limited data. DoD organizations should include DSN numbers where noted.

- Non-DoD Government organizations complete only Section I if requesting access to only unclassified/unlimited data.

(2) Section II - Security Officer. All U.S. Government organizations requesting access to classified data must obtain the signature of their organization's security officer. The security officer certifies that the organization listed in Section I may receive and store classified data at the access level indicated in Section I (Item 11, "Type of Access Desired").

(3) Section III - Prime Contractor Approval. Leave blank.

(4) Section IV - U.S. Government Approving Official. DoD organizations must complete Section IV if requesting access to classified data. Non-DoD Government organizations must complete Section IV if requesting access to unclassified/limited or classified data. Signature of Government Approving Official is required.

- Approving Official for DoD organizations is any designated official, such as the Commanding Officer, Technical Director, etc.

- Non-DoD Government organizations refer to DTIC's registration guide for the address of their approving official.

(5) Section V - Subject Fields and Groups. All U.S. Government organizations requesting access to classified data must select the pertinent subject fields of interest based on user need-to-know requirements.

**2. Contractors, Subcontractors, Potential Contractors, CRDA Partners, and Grantees**

Access to export-controlled data requires DTIC's receipt of a certified copy of the DD Form 2345, "Militarily Critical Technical Data Agreement." Access to classified data requires approved facility clearance from the Defense Investigative Service (DIS). For more information, refer to DTIC's registration guide.

(1) Section I - General Information. All contractors, subcontractors, and potential contractors must complete Section I in full. Cite your prime contract number and expiration date in this section.

(2) Section II - Security Officer. Leave blank.

(3) Section III - Prime Contractor Approval. All subcontractors must complete Section III. Cite your subcontract number and expiration date in this section.

(4) Section IV - U.S. Government Approving Official. All contractors, subcontractors, and potential contractors must complete Section IV. Signature of Government approving official is required. (Refer to DTIC's registration guide for information on who may qualify as the approving official.)

(5) Section V - Subject Fields and Groups. All contractors, subcontractors, and potential contractors requesting access to classified data must select the pertinent subject fields of interest based on user need-to-know requirements.

**E. AFTER REGISTRATION**

(1) DTIC will mail a numeric user code and additional information to the user upon completion of registration.

(2) Registered DTIC users must notify DTIC in writing of any changes to their current DD Forms 1540.

(3) Registered DTIC users receive a notice from DTIC 60 days prior to the scheduled expiration date of their service.

**F. ADDITIONAL INFORMATION**

For a more complete instructional guide, refer to the "Registration Guide to the Defense Technical Information Center (DTIC)." Copies may be obtained from the address in Paragraph B.

# REGISTRATION FOR SCIENTIFIC AND TECHNICAL INFORMATION SERVICES

Form Approved  
OMB No. 0704-0264  
Expires May 31, 1998

Public reporting burden for this collection of information is estimated to average 26 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0264), Washington, DC 20503.

**PLEASE DO NOT RETURN YOUR FORM TO EITHER OF THESE ADDRESSES. SEND YOUR COMPLETED FORM TO: DEFENSE TECHNICAL INFORMATION CENTER, ATTN: DTIC-BCS, 8725 JOHN J. KINGMAN ROAD, SUITE 0944, FORT BELVOIR, VA 22060-6218.**

## SECTION I - GENERAL INFORMATION (All applicants must complete Section I.)

1. ORGANIZATION NAME				2. SUBORGANIZATION NAME				FOR DTIC USE ONLY																											
3.a. STREET ADDRESS				b. CITY		c. STATE		d. ZIP CODE		DTIC USER CODE																									
4. ATTENTION				5. TELEPHONE NUMBER (Include area code)				6. FAX NUMBER (Include area code)				RENEWAL DATE (YYMMDD)																							
a. NAME (Last, First, Middle Initial)				b. POSITION/TITLE				c. OFFICE SYMBOL				USER TYPE																							
a. COMMERCIAL				b. DSN		a. COMMERCIAL		b. DSN		CHARGE CODE		ENTITY CODE		SERVICE LEVEL SPONSOR		CAGE CODE																			
7. INTERNET E-MAIL ADDRESS				8.a. PRIME CONTRACT NUMBER (Or other appropriate number) (Contractors only)				b. EXPIRATION DATE (YYMMDD)				FACILITY SECURITY CLEARANCE																							
9. CURRENT OR FORMER USER (X one)				10. MILITARILY CRITICAL TECHNICAL DATA AGREEMENT				11. TYPE OF ACCESS DESIRED (X as applicable)				SECURITY CLEARANCE																							
<input type="checkbox"/> YES (Enter DTIC user code)				<input type="checkbox"/> NO				<input type="checkbox"/> UNCLASSIFIED/UNLIMITED				<input type="checkbox"/> UNCLASSIFIED/LIMITED				<input type="checkbox"/> CONFIDENTIAL				<input type="checkbox"/> SECRET				<input type="checkbox"/> RESTRICTED DATA				<input type="checkbox"/> CNWDI				<input type="checkbox"/> NATO			
				CERTIFICATION NUMBER (Contractors only)				TYPE				RD				CNWDI SIGMA				NATO															

## SECTION II - SECURITY OFFICER (All U.S. Government organizations must complete Section II if requesting access to classified data.)

12. SECURITY OFFICER CERTIFICATION  
I certify that the organization listed in Section I may receive and store classified data at the access level indicated in Section I.

a. NAME (Last, First, Middle Initial)				b. ORGANIZATION NAME							
c. (1) STREET ADDRESS				(2) CITY		(3) STATE		(4) ZIP CODE			
d. TELEPHONE NUMBER (Include area code)				e. SIGNATURE				f. DATE SIGNED (YYMMDD)			
(1) COMMERCIAL		(2) DSN									

## SECTION III - PRIME CONTRACTOR APPROVAL (All subcontractors must complete Section III. Prime Contractor's signature is required.)

13. PRIME CONTRACTOR ORGANIZATION NAME				14.a. SUBCONTRACT NUMBER				b. EXPIRATION DATE (YYMMDD)			
15.a. STREET ADDRESS				b. CITY				c. STATE		d. ZIP CODE	
16.a. PRIME CONTRACTING OFFICER NAME (Last, First, Middle Initial)				b. POSITION/TITLE							
c. TELEPHONE NUMBER (Include area code)		d. SIGNATURE				e. DATE SIGNED (YYMMDD)					

## SECTION IV - U.S. GOVERNMENT APPROVING OFFICIAL (All contractors, those DoD organizations requesting access to classified data, and Non-DoD Government organizations requesting access to unclassified/limited or classified data must complete Section IV. Government Approving Official's signature is required.)

17. APPROVING ORGANIZATION NAME				18.a. STREET ADDRESS				b. CITY		c. STATE		d. ZIP CODE	
18.a. APPROVING OFFICIAL NAME (Last, First, Middle Initial)				b. POSITION/TITLE									
c. TELEPHONE NUMBER (Include area code)				d. SIGNATURE				e. DATE SIGNED (YYMMDD)					
(1) COMMERCIAL		(2) DSN											

FOR DTIC USE ONLY

**SECTION V SUBJECT FIELDS AND GROUPS** *(X as applicable. All applicants must complete Section V if requesting access to classified data. The first number is the subject field, the second is the more specific group.)*

01 Aviation Technology (ALL)	11 Materials (Continued)	18 Nuclear Science & Technology (ALL)
01 Aerodynamics	03 Coatings, Colorants & Finishes	01 Fusion Devices (Thermonuclear)
02 Military Aircraft Operations	04 Laminates & Composite Materials	02 Isotopes
03 Aircraft	06 Textiles	03 Nuclear Explosions & Devices (Non-Military)
03.01 Helicopters	08 Metallurgy & Metallography	04 Nuclear Instrumentation
03.02 Bombers	06.01 Properties of Metals & Alloys	05 Nuclear Power Plants & Fusion Reactor Engineering
03.03 Attack and Fighter Aircraft	06.02 Fabrication Metallurgy	05.01 Nuclear Fusion Reactors (Power)
03.04 Patrol & Reconnaissance Aircraft	07 Miscellaneous Materials	05.02 Nuclear Fusion Reactors (Non-Power)
03.06 Transport Aircraft	08 Lubricants & Hydraulic Fluids	06 Nuclear Radiation Shielding Protection & Safety
03.06 Training Aircraft	09 Plastics	07 Radioactivity, Radioactive Wastes & Fusion Products
03.07 V/STOL	10 Elastomers & Rubber	08 SNAP (Systems for Nuclear Auxiliary Power) Technology
03.08 Gliders and Parachutes	11 Solvents, Cleaners & Abrasives	09 Fusion Reactor Physics
03.09 Civilian Aircraft	12 Wood, Paper & Related Forestry Products	10 Fusion Reactor Materials
03.10 Pilotless Aircraft	12 Mathematical & Computer Science (ALL)	19 Ordnance (ALL)
03.11 Lighter-than-Air Aircraft	01 Numerical Mathematics	01 Ammunition & Explosives
03.12 Research & Experimental Aircraft	02 Theoretical Mathematics	01.01 Pyrotechnics
04 Flight Control & Instrumentation	03 Statistics & Probability	02 Aerial Bombs
05 Terminal Flight Facilities	04 Operations Research	03 Combat Vehicles
06 Commercial & General Aviation	05 Computer Programming & Software	04 Armor
02 Agriculture (ALL)	06 Computer Hardware	05 Fire Control & Bombing Systems
01 Agricultural Chemistry	07 Computer Systems	06 Guns
02 Agricultural Economics	08 Computer Systems Management & Standards	07 Rockets
03 Agricultural Engineering	09 Cybernetics	08 Underwater Ordnance
04 Agronomy, Horticulture, & Aquaculture	13 Mechanical, Industrial, Civil & Marine Engineering (ALL)	08.01 Torpedoes
05 Animal Husbandry & Veterinary Medicine	01 Air Conditioning, Heating, Lighting & Ventilating	09 Explosives
06 Forestry	02 Civil Engineering	10 Ballistics
03 Astronomy & Astrophysics (ALL)	03 Construction Equipment, Materials & Supplies	11 Nuclear Weapons
01 Astronomy	04 Containers & Packaging	12 Directed Energy Weapons
02 Astrophysics	05 Couplers, Fasteners & Joints	13 Guided Munitions
03 Celestial Mechanics	06 Surface Transportation & Equipment	20 Physics (ALL)
04 Atmospheric Sciences (ALL)	06.01 Surface Effect Vehicles/Amphibious Vehicles	01 Acoustics
01 Atmospheric Physics	07 Hydraulic & Pneumatic Equipment	02 Crystallography
02 Meteorology	08 Manufacturing & Industrial Engineering & Control of Production Systems	03 Electricity & Magnetism
05 Behavioral & Social Science (ALL)	09 Machinery & Tools	04 Fluid Mechanics
01 Administration & Management	10 Marine Engineering	05 Atomic & Molecular Physics & Spectroscopy
02 Information Science	10.01 Submarine Engineering	06 Optics
03 Economics & Cost Analysis	11 Pumps, Filters, Pipes, Tubing, Fittings & Valves	06.01 Fiber Optics & Integrated Optics
04 Government & Political Science	12 Safety Engineering	07 Particle Accelerators
05 Sociology & Law	13 Structural Engineering & Building Technology	08 Nuclear Physics & Elementary Particle Physics
06 Humanities & History	14 Test Equipment, Research Facilities & Reprography (ALL)	09 Plasma Physics & Magnetohydrodynamics
07 Linguistics	01 Holography	10 Quantum Theory & Relativity
08 Psychology	02 Test Facilities, Equipment & Methods	11 Mechanics
09 Personnel Management & Labor Relations	03 Recording & Playback Devices	12 Solid State Physics
06 Biological & Medical Science (ALL)	04 Photography	13 Thermodynamics
01 Biochemistry	05 Printing & Graphic Arts	14 Radiofrequency Wave Propagation
02 Genetic Engineering & Molecular Biology	15 Military Science (ALL)	15 Electromagnetic Pulses
03 Biology	01 Military Forces & Organizations	21 Propulsion, Engines & Fuels (ALL)
04 Anatomy & Physiology	02 Civil Defense	01 Air Breathing Engines (Unconventional)
05 Medicine & Medical Research	03 Defense Systems	02 Combustion & Ignition
06 Ecology	03.01 Antimissile Defense Systems	03 Electric & Ion Propulsion
07 Radiobiology	03.02 Antiaircraft Defense Systems	04 Fuels
08 Food, Food Service & Nutrition	03.03 Antisatellite Defense Systems	05 Jet & Gas Turbine Engines
09 Hygiene & Sanitation	04 Military Intelligence	06 Nuclear Propulsion
10 Stress Physiology	05 Logistics, Military Facilities & Supplies	07 Reciprocating & Rotating Engines
11 Toxicology	06 Military Operations, Strategy & Tactics	08 Rocket Engines
12 Medical Facilities, Equipment & Supplies	06.01 Naval Surface Warfare	08.01 Liquid Propellant Rocket Engines
13 Microbiology	06.02 Undersea & Antisubmarine Warfare	08.02 Solid Propellant Rocket Engines
14 Weapons Effects (Biological)	06.03 Chemical, Biological & Radiological Warfare	09 Rocket Propellants
15 Pharmacology	06.04 Nuclear Warfare	09.01 Liquid Rocket Propellants
07 Chemistry (ALL)	06.05 Space Warfare	09.02 Solid Rocket Propellants
01 Industrial Chemistry/Chemical Processing	06.06 Land Mine Warfare	22 Space Technology (ALL)
02 Inorganic Chemistry	06.07 Unconventional Warfare	01 Astronauts
03 Organic Chemistry	18 Guided Missile Technology (ALL)	02 Unmanned Spacecraft
04 Physical Chemistry	01 Guided Missile Launching & Basing Support	03 Spacecraft Trajectories and Reentry
05 Radiation & Nuclear Chemistry	02 Guided Missile Trajectories, Accuracy & Ballistics	04 Ground Support Systems & Facilities for Space Vehicles
06 Polymer Chemistry	02.01 Guided Missile Dynamics, Config. & Control Surfaces	05 Manned Spacecraft
08 Earth Science & Oceanography (ALL)	03 Guided Missile Warheads & Fuzes	23 Biotechnology (ALL)
01 Biological Oceanography	04 Guided Missiles	01 Biomedical Instrumentation & Bioengineering
02 Cartography & Aerial Photography	04.01 Air- & Space-Launched Guided Missiles	02 Human Factors Engineering & Man Machine Systems
03 Physical & Dynamic Oceanography	04.02 Surface-Launched Guided Missiles	03 Bionics
04 Geomagnetism	04.03 Underwater-Launched Guided Missiles	04 Protective Equipment
05 Geodesy	05 Guided Missile Reentry Vehicles	05 Life Support Systems
06 Geography	17 Navigation, Detection & Countermasures (ALL)	06 Escape, Rescue & Survival
07 Geology, Geochemistry & Mineralogy	01 Acoustic Detection & Detectors	24 Environmental Pollution & Control (ALL)
08 Hydrology, Limnology & Potamology	02 Non-Acoustic/Non-Magnetic Submarine Detection	01 Air Pollution & Control
09 Mining Engineering	03 Direction Finding	02 Noise Pollution & Control
10 Soil Mechanics	04 Countermasures	03 Solid Waste Pollution & Control
11 Seismology	04.01 Radio Countermasures	04 Water Pollution & Control
12 Snow, Ice, & Permafrost	04.02 Acoustic Countermasures	05 Pesticides Pollution & Control
09 Electrotechnology & Fluidics (ALL)	04.03 Radar Countermasures	06 Radiation Pollution & Control
01 Electrical & Electronic Equipment	04.04 Optical Countermasures	07 Environmental Health & Safety
02 Fluidics & Fluorics	05 Optical Detection & Detectors	26 Communications (ALL)
03 Lasers & Masers	05.01 Infrared Detection & Detectors	01 Telemetry
04 Line, Surface & Bulk Acoustic Wave Devices	05.02 Ultraviolet Detection & Detectors	02 Radio Communications
05 Electrooptical & Optoelectronic Devices	06 Magnetic & Electric Field Detection & Detectors	03 Non-Radio Communications
06 Acousto-optical & Optoacoustic Devices	07 Navigation & Guidance	04 Voice Communications
07 Electromagnetic Shielding	07.01 Land & Riverine Navigation & Guidance	05 Command, Control & Communications Systems
10 Power Propulsion & Energy Conversion (Nonpropulsive) (ALL)	07.02 Underwater & Marine Navigation & Guidance	ALL ALL SUBJECT FIELDS AND GROUPS
01 Non-Electrical Energy Conversion	07.03 Air Navigation & Guidance	
02 Electric Power Production & Distribution	07.04 Space Navigation & Guidance	
03 Electrochemical Energy Storage	08 Miscellaneous Detection & Detectors	
04 Energy Storage	09 Active & Passive Radar	
11 Materials (ALL)	10 Seismic Detection & Detectors	
01 Adhesives, Seals & Binders	11 Target Direction, Range & Position Finding	
02 Ceramics, Refractories & Glass		
02.01 Refractory Fibers		

# CONTRACT DATA REQUIREMENTS LIST

(1 Data Item)

**Form Approved**  
**OMB No. 0704-0188**

Public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project, (0704-0188), Washington, DC 20503. Please DO NOT RETURN your form to either of these addresses. Send completed form to the Government issuing Contracting Officer for the Contract PR No. listed in Block E.

A. CONTRACT LINE ITEM NO.	B. EXHIBIT	C. CATEGORY: TDP _____ TM- _____ OTHER _____ S (SECURITY)	
---------------------------	------------	--	--

D. SYSTEM/ITEM	E. CONTRACT / PR NO.	F. CONTRACTOR
----------------	----------------------	---------------

1. DATA ITEM NO.	2. TITLE OF DATA ITEM <b>OPERATIONS SECURITY (OPSEC) PLAN</b>	3. SUBTITLE
------------------	--	-------------

4. AUTHORITY (Data Acquisition document No.) <b>DI-MGMT-80934</b>	5. CONTRACT REFERENCE	6. REQUIRING OFFICE <b>NAWCAD 7.4.4</b>
--	-----------------------	--

7. DD 250 REQ.	9. DIST STATEMENT REQUIRED <b>B</b>	10. FREQUENCY	12. DATE OF FIRST SUBMISSION	14. DISTRIBUTION		
8. APP CODE	11. AS OF DATE	13. DATE OF SUBSEQUENT SUBMISSION	a. ADDRESSEE <b>744000A</b>		b. COPIES Draft      Final Reg      Reg      Regro	
				<b>1</b>	<b>1</b>	<b>0</b>

16. REMARKS

**Block 4: Delete references in DI-MGMT-80934. Instead use the definition of sensitive information given in Public Law 100-235; use National Security Directive (NSSD) 298 for the concept of Operations Security.**

**Block 9: Apply and use distribution statements in accordance with the Distribution Statement Attachment to this contract. See SECNAVINST 5510.36, Chapter 8 for guidance.**

**Blocks 11, 12 & 13: Preliminary draft plan due 90 days DAC. Final due 45 days after government approval of draft. Revisions are required after approval of final plan only to comply with Government Data Protection Policy Documents revision.**

15. TOTAL →	1	1	0
-------------	---	---	---

G. PREPARED BY	H. DATE	I. APPROVED BY	J. DATE
----------------	---------	----------------	---------

17. PRICE GROUP
18. ESTIMATED TOTAL PRICE

# DATA ITEM DESCRIPTION

Form Approved  
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 110 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. TITLE  OPERATIONS SECURITY (OPSEC) PLAN	2. IDENTIFICATION NUMBER  DI-MGMT-80934
--	---

3. DESCRIPTION / PURPOSE  3.1 The OPSEC Plan describes the methods to: (1) Identify OPSEC security responsibilities and requirements, (2) Define overall OPSEC security standard practice procedures, (3) Identify potential problem areas and determine solutions, and (4) Develop OPSEC security awareness inputs into the overall system security process.  3.2 The Plan is utilized to identify and monitor a contractor's OPSEC activities during performance of the contract.
---

4. APPROVAL DATE (YYYYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR)  NAWCAD 7.4.4	6a. DTIC APPLICABLE	6b. GIDEP APPLICABLE
--------------------------------	---	---------------------	----------------------

7. APPLICATION / INTERRELATIONSHIP  7.1 This DID contains the format and content preparation instructions for the data product generated by the specific and discrete task requirements delineated in the contract. 7.2 The DID is applicable only when the contracting activity determines that the sensitivity of the contract warrants the effort. 7.3 The initial submission may be broad in scope; however, the level of detail increases as the work progresses to the point that any security-related question will be addressed in the Plan. 7.4 The contractor's implementation of the OPSEC Plan, approved by the contracting agency, is also subject to joint inspection by the Defense Security Service and the contracting agency.
--

8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER
------------------------	----------------------	-----------------

10. PREPARATION INSTRUCTIONS 10.1 REFERENCE DOCUMENTS: The applicable issue of the document cited herein, including their approval dates and dates of any applicable amendments, notices and revisions shall be as specified in the contract. 10.2 FORMAT: The OPSEC Plan format shall be contractor selected. Unless effective presentation would be degraded the initially used format arrangement shall be used for all subsequent submissions. 10.3 CONTENT: The OPSEC Plan shall include the results of the five-step OPSEC analysis described therein including those applicable to the specific contract. 10.3.1 GENERAL: The OPSEC Plan shall contain details of the OPSEC management concept to include contract identification, assignment of responsibilities, definition of milestones with target dates, provisions for continuous analysis, and periodic revision as the contract activities evolve and become more specific and detailed. 10.3.2: THREAT: The OPSEC Plan shall contain the threat provided by the contracting activity 'applicable to the specific contract activities. 10.3.3: SENSITIVE ASPECTS OF THE CONTRACT: The OPSEC Plan shall contain an overview of all activities, operations, tests, etc. to be undertaken in the performance of the contract; identify those in which classified information will manifest itself; identify the topics of the classification guide that specify the information is classified; determine how, where, and when the classified information is embodied in the hardware, software, or operations; determine what type access (visual, physical, possession, etc.) permits knowledge of the classified information, what tools/equipment/capability are required, and the specific national defense advantage provided by the information if it is protected. Based on the above analysis, an Essential Elements of Friendly Information (EEFI) List shall be prepared. This list is to include all the information considered "essential" to the success of the effort, all the information that must be protected to preserve the military advantage potentially provided by the effort. Additionally, the list shall include all the activities, operations, tests, etc. that could reveal the "essential" information to foreign intelligence services (FIS). 10.3.4 VULNERABILITIES: The OPSEC Plan shall contain vulnerabilities derived by comparing threat to sensitive activities to determine which sensitive activities can be observed by FIS. "Observe" is defined to include all physical and chemical properties that can be noted and recorded by any type of sensor to include TEMPEST concerns. The instructions in the Industrial OPSEC Guide shall be followed to identify potential TEMPEST vulnerabilities. 10.3.5 COUNTERMEASURES: The OPSEC Plan shall include the protective measure deemed appropriate for each vulnerability.
---

11. DISTRIBUTION STATEMENT  DISTRIBUTION STATEMENT B.
---

## SECTION C - LANGUAGE

Item XXXX - The OPSEC program to be furnished under this Item will be furnished pursuant to the requirements provided herein:

- a. The contractor is required to provide Operations Security (OPSEC) protection for all classified information and sensitive information, pursuant to the National Security Decision Directive 298 of 22 January 1988. The current editions of DoD Manual 5200.1-R and OPNAVINST 3432 shall be used as guidance. In order to meet this requirement, the contractor shall develop, implement, and maintain a facility level OPSEC program in accordance with exhibit \_\_\_\_ to protect classified and sensitive information to be used at a contractor's and subcontractor's facilities during the performance of this contract.
- b. The Contractor is responsible for subcontractor implementation of the OPSEC program requirements for this contract.

Item XXXX - The data called for hereunder shall be provided in accordance with the Exhibit \_\_\_\_\_. The contractor's OPSEC program is to be described in a facility level OPSEC\* planning document. The contractor will submit the document to the Government for approval.

\*Note: If an option other than a facility level OPSEC plan is selected for this contract, replace "facility level OPSEC" with the appropriate option.

***DRAFT ONLY***

**OPERATIONS SECURITY (OPSEC) PLAN**

**FOR THE**

**(PROGRAM/PROJECT)**

**CONTRACT NO. xxxxxxxxxxxxxx**

**CDRL REFERENCE NO. XXXX**

**DATE:**

**SUBMITTED TO:**

**PREPARED BY:**

**DISTRIBUTION STATEMENT  
FOR OFFICIAL USE ONLY**

***DRAFT ONLY***

***TABLE OF CONTENTS***

<b><u>Paragraph</u></b>	<b><u>Title</u></b>	<b><u>Page</u></b>
1.0	Purpose	
2.0	Policy	
3.0	Scope	
4.0	Background	
5.0	Responsibilities	
6.0	Operations Security (OPSEC)	
6.1	Critical Information	
6.2	Threat	
6.3	Vulnerabilities	
6.4	Risk Assessment	
6.5	Countermeasures	
7.0	FOR OFFICIAL USE ONLY/Sensitive Information	
8.0	Public Release	
9.0	Education and Awareness	
10.0	Point of Contact	

**FOR OFFICIAL USE ONLY**

***DRAFT ONLY***

## ***Operations Security Plan***

### **1.0 Purpose**

(Usually to establish an OPSEC program for the organization and to direct its implementation.)

### **2.0 Policy**

(State the policy of the organization with regard to protection of information)

### **3.0 Scope**

(What the program includes, i.e., classified and unclassified programs; list exceptions, if any.)

### **4.0 Background**

(Program description and parties involved, i.e., NAWCAD PAX, prime contractor, subcontractors)

### **5.0 Responsibilities**

(OPSEC is the responsibility of everyone assigned to the program. Who is responsible for the overall OPSEC program and who will be responsible for implementation and monitoring of all aspects including revisions and training.)

### **6.0 Operations Security (OPSEC)**

(Basic OPSEC philosophy and approach)

What is OPSEC?

OPSEC is a systematic and proved process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities. The OPSEC process is most effective when fully integrated into all planning and operational processes. The OPSEC process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risk, and application of appropriate countermeasures.

Generally unclassified evidence of the planning and execution of sensitive Government activities could include otherwise unprotected engineer and computer science networking; technology development; technology application(s); and RDT&E thrusts. Other sensitive information that could provide adversaries with insight to critical secrets could include such events as part ordering; prime and subcontractor communications; test and evaluation; and shipping of deliverables. OPSEC usually is concerned with those necessary peripheral actions and events that must occur, but which may also provide a tip-off to the adversary. OPSEC applications rarely affect what occurs, but does affect how things occur, and can be of enormous help in the planning process. OPSEC does not evaluate the effectiveness of traditional security countermeasures. Rather, it assumes that such measures are in place and effective, and concentrates on what is unprotected by those measures.

#### **6.1 Critical Information**

(Critical Information is information about friendly intentions, capabilities, or activities that must be protected from loss to keep an adversary from gaining a significant military, economic, political, or technological advantage. The process begins with an examination of the totality of an activity to determine what exploitable but unclassified evidence of classified or sensitive activity is vulnerable to adversary

**FOR OFFICIAL USE ONLY**

## ***DRAFT ONLY***

acquisition in light of the known collection capabilities of potential adversaries. Such evidence is usually derived from openly available data. Certain indicators may be pieced together or interpreted to discern critical information. Indicators commonly stem from the routine administrative, physical, or technical actions taken to prepare for or execute a plan or activity. This section should include, but also expand upon, the data provided by the government sponsor. It should include critical information relating to such things as manufacturing processes or proprietary data or operations that could allow an adversary necessary data to acquire the critical information specified by the government sponsor.)

### **6.2 Threat**

(The plan should contain the threat information provided by the government and any other pertinent information known to the program or activity officials specifying known threat to their location, personnel, information, or operations. Threat should be tailored to both the information and locations identified as critical to the sponsor and the program or activity. An essential part of this section should be a thorough analysis of the available open-source information concerning both the program/activity's and sponsor's operations in similar efforts and technologies. The threat to U.S. Government activities continues. The political changes that took place in eastern Europe have certainly changed the focus of U.S. concerns from a nuclear-centered threat to an economic-centered threat, but the potential for grave harm to the U.S. continues. Although it is a less cataclysmic climate, the ultimate result is the same. Information about specific adversary capabilities is available from the NAWCAD OPSEC Officer. This includes, but not limited to, information on organizations such as the Russian Foreign Intelligence Service (SVRR); People's Republic of China (PRC); Intelligence services of countries friendly to U.S. interests; competitors in the economic world; or efforts by narcotraffickers or terrorist groups.)

### **6.3 Vulnerabilities**

(OPSEC vulnerabilities are normally found in the processes and procedures routinely used by organizations. This section should discuss the process by which vulnerabilities to critical information will be determined. This section will become more focused as the program/activity matures. This part of the plan will require periodic updating based on new threat information and changes in the scope of the program/activity. Determining vulnerabilities involves a systematic analysis of how an operation or activity is actually conducted by the primary and supporting organizations. The organization and activity must be viewed as an adversary might view it. Actions and things that can be observed, or other data that can be interpreted or pieced together to drive critical information, must be identified. These potential vulnerabilities must be matched with specific threats. Once you determine what an adversary needs to know and where that information is available, it is necessary to determine if it is possible that the adversary could acquire and exploit the information in time to capitalize on it. If so, a vulnerability exists.)

### **6.4 Risk Assessment**

(This section should document the requirement for and the process of evaluating the threats to and vulnerabilities of the program/activity. It should be remembered that the purpose of risk assessment is to give an educated opinion or calculation on the probability of critical information loss and its impact, as a guide in taking action. Risk Assessment is essentially the process of balancing a vulnerability against the threat, the deciding if the resultant risk warrants application of countermeasures. The determination of risk is a demanding step in the OPSEC process. It requires a degree of subjective decision making based on the best estimate of an adversary's intentions and capabilities. Included in the assessment of an adversary's capability is not only his ability to collect the information but also his capability to process and exploit (evaluate, analyze, interpret) in time to make use of the information. In order to complete the risk assessment, it is necessary to combine this information (i.e., the possibility of the adversary exploiting the information, with the resultant impact on the organization or program). This process should result in a list of recommendations along with an estimate of the reduced impact upon the operation achieved through their application. The decision maker can then weigh the cost of recommended OPSEC measures in terms of resources and operational effectiveness against the impact of the loss of the critical information.)

**FOR OFFICIAL USE ONLY**

# ***DRAFT ONLY***

## **6.5 Countermeasures**

(For each identified vulnerability, a short list of potential countermeasures should be developed. A detailed assessment of the cost of implementing each countermeasure, the possible impact of not implementing, and appropriate milestones should be provided. Cost should include both direct and indirect monetary impacts. Measures such as cover, counterimagery, and deception may also be recommended. It should be noted, however, that some measures are very costly. A countermeasure is anything that effectively negates an adversary's ability to exploit vulnerabilities. the most effective countermeasures are simple, straightforward, procedural adjustments that effectively eliminate or minimize the generation of indicators. Following a cost-benefit analysis, countermeasures are implemented in priority order to protect vulnerabilities having the most significant impact on the organization, as determined by the appropriate decision maker.

## **7.0 FOR OFFICIAL USE ONLY/Sensitive Information**

FOR OFFICIAL USE ONLY and/or sensitive information control, destruction, transmission, dissemination, storage, and marking requirements must be stated. This information must be secured in a locked office, desk, cabinet, and/or facility. Open storage or unlimited access by individuals at any location is not authorized (normally, corporate proprietary information control procedures are sufficient).

## **8.0 Public Releases**

Any public release of information must be approved by the NAWC OPSEC Officer and the Public Affairs Officer. Public release is, but not limited to, publication of articles in sales medium or media, World Wide Web, symposia, conferences, etc. involving DoD programs/projects or activities.

## **9.0 Education and Awareness**

(Outline how you will educate your employees about OPSEC and this Plan. This training must be accomplished at least once a year. How will you document this training and who is responsible.)

## **10.0 Point of Contacts**

(Who is the focal point in your company for OPSEC (working level))

**FOR OFFICIAL USE ONLY**