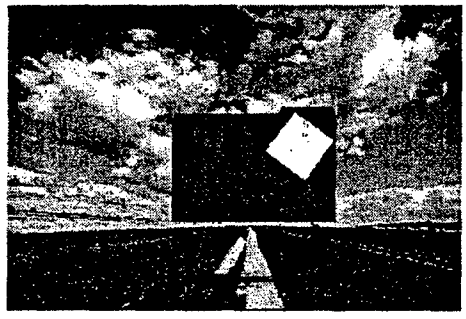
How to Overcome Information Anxiety:

Marking DoD Technical Documents for Distribution



Participant Manual

Prepared for the

Office of Scientific and Technical Information Policy
U.S. Department of Defense

Prepared by the

Oak Ridge Institute for Science and Education

May 1998

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
May 1998	Participant Manual	

4. TITLE AND SUBTITLE
How to Overcome Information Anxiety
Assignment and Use of DoD Distribution Statements for Technical Documents
Vol. 2
Participant Manual

5a. CONTRACT NUMBER
DE-AC05-76OR00033

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Oak Ridge Institute for Science and Education (ORISE)
ETD-Mitchell Road
ORISE
P.O. Box 117
Oak Ridge, TN 37831-0117

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
DoD Office of Scientific and Technical Information Policy
Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)
DTIC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
TR--2000/7-V2

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Vol. 2 is the Participant Manual for this training course.
Vol. 1 is the Facilitator Guide for this training course. See **AD-A379 183** for Vol. 1.

14. ABSTRACT
This course on DoD distribution statements is in two volumes. The Participant Guide contains a set of the instructor's slides and reference materials. The course is intended to offer DoD staff and contractors a basic understanding of the rationale and mechanics of properly assigning distribution statements to DoD technical documents. While other markings are applied to DoD technical documents, this course only covers distribution statements.

15. SUBJECT TERMS: Distribution statements; distribution limitations; document markings; document preparation; scientific and technical information; STINFO; information security; security training; unclassified but sensitive; controlling technical documents.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
	Unclassified				STINFO Training Office
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
Unclassified	Unclassified	Unclassified	UU	296	(703) 767-8208 (703) 767-8240

Table of Contents

Foreword.....ii

Pre-Training Survey..... iv

Module 1.....PG 1-1

Module 2.....PG 2-1

Module 3.....PG 3-1

Module 4.....PG 4-1

Post-Training Survey

References

3200.12 *DoD Scientific and Technical Information (STI) Program (STIP)*

5220.22 *DoD Industrial Security Program*

5230.9 *Clearance of DoD Information for Public Release*

5230.29 *Security and Policy Release*

5230.11 *Disclosure of Classified Military Information to Foreign Governments and International Organizations*

5230.24 *Distribution Statements on Technical Documents*

5230.25 *Withholding of Unclassified Technical Data from Public Disclosure*

5400.7 *DoD Freedom of Information Act Program*

5400.11 *DoD Privacy Program*

8910.1 *Management and Control of Information Requirements*

EO 12958 *Classified National Security Information*

National Policy on Protection of Sensitive, But Unclassified Information In Federal Government Telecommunications and Automated Information Systems

Defense Acquisition Circular 91-11, Subpart 227.71 – Rights in Technical Data

Continuation of Export Control Regulations (from the White House Virtual Library)

Arms Export Control Act

FOREWORD

The Department of Defense Office of Scientific and Technical Information Policy designed and developed this training course to meet the needs of Defense personnel and contractors who play roles in the creation and management of Defense scientific and technical data, documents, and information. The specific focus of this course is the assignment and use of DoD Distribution Statements, as required by DoD Directive 5230.24.

The needs assessment that preceded course development identified great variation in practice among organizations. Specific problems and concerns mentioned by the individuals interviewed and subsequently addressed in the training include the following:

- Lack of familiarity with the policies that require Distribution Statements
- Lack of understanding of the reasons for the policies
- Uncertainties about what *is* scientific and technical information and what *is not*
- Lack of clarity in the division of responsibility between the "Controlling Office" and the performer of the work
- Uncertainties as to who should be making decisions about distribution of technical documents when contractors are engaged in research and other activities
- Difficulty in balancing the need for restrictions against the need for dissemination
- Preferences institutionalized in some groups for particular distribution levels ("We always use B")
- Failure to mark classified documents and sometimes simple failure to mark documents at all
- Problems with assigning a Distribution Statement years after a document was created (e.g., during declassification)
- Dealing with requests for exceptions

Some personnel reported that they dealt with Distribution Statements only infrequently, while others have assumed new responsibilities in this area as a result of such organizational changes as downsizing and reorganization.

To help staff overcome these and other barriers to correctly assigning Distribution Statements, this course and its supporting resources were developed with an overall objective of providing a basic understanding of DoD policies and the major issues, merits, rationale, and mechanics of properly assigning Distribution Statements to DoD technical documents, data, and information.

The goals for participants in the training are to:

- Understand the principles of DoD policy guiding decisions on Distribution Statements, and specifically, which issues are important given the materials each participant routinely handles.

- Recognize the variables that must be considered with each document, drawing, data set, or other body of information, and some of the complexities personnel may encounter.

- Be able to demonstrate the process for correctly assigning Distribution Statements to DoD technical information, data, and documents with the help of take-home materials and job aids.

This Page Intentionally Left Blank

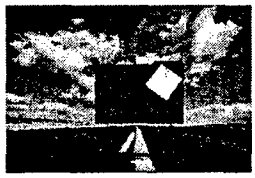
Module 1

This Page Intentionally Left Blank

Assignment and Use of DoD Distribution Statements for Technical Documents

How to Overcome Information Anxiety...

about DoD Distribution Statements



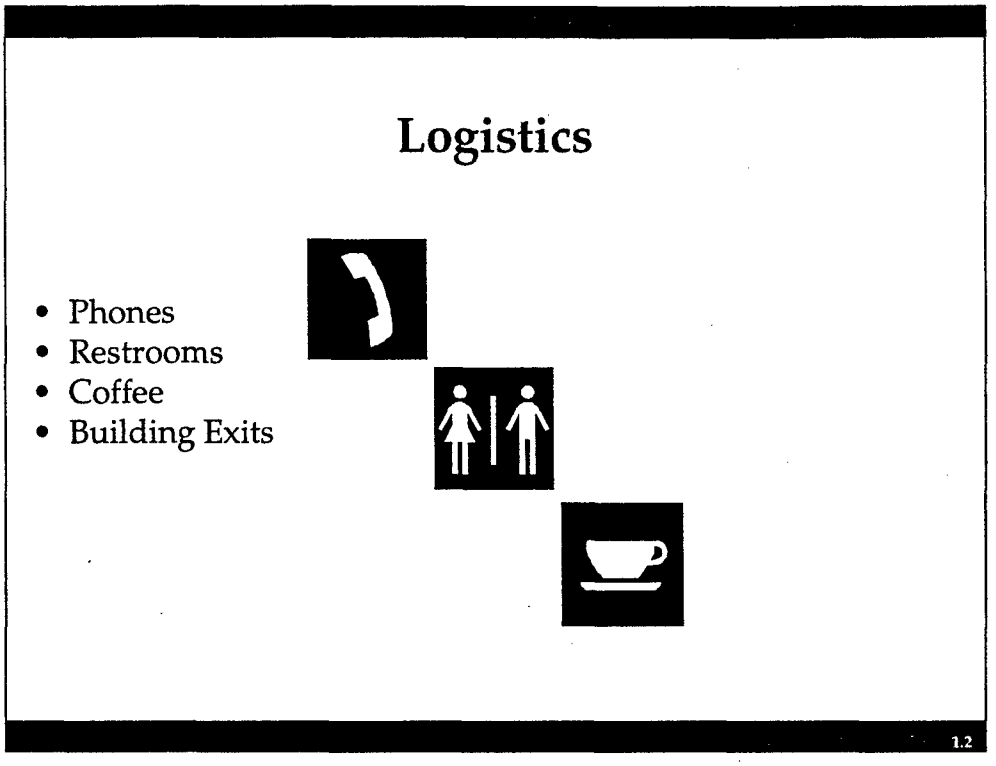
Offered by the

Office of Scientific and Technical Information Policy

U.S. Department of Defense

1. Getting Started and Getting Motivated 1.1

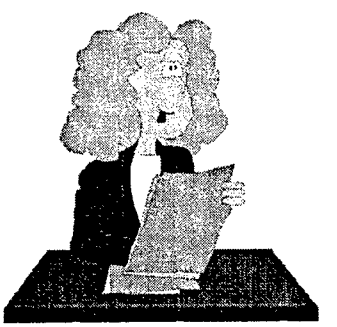
Notes:



Notes:

Course Objective

- To provide a basic understanding of DoD policies and the major issues, merits, rationale, and mechanics of properly assigning Distribution Statements to DoD technical documents.



1.3

Notes:

By the End of This Course, You Should:

- Understand the principles of DoD policy guiding decisions on Distribution Statements, and specifically, which issues are important given the materials you routinely handle.
- Recognize the variables you must consider with each document, drawing, data set, or other body of information, and some of the complexities you may encounter.
- Be able to demonstrate the process for (correctly!) assigning Distribution Statements to DoD technical information, data, and documents with the help of materials and job aids you will take home from this session.

1.4

Notes:

Module 1 Objective

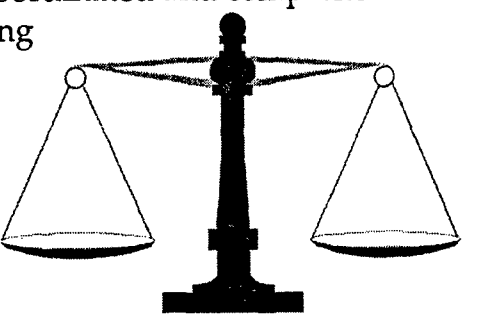
- Participants will be able to describe the purpose and benefits of DoD's policy on marking and distributing DoD technical documents, information, and data.

1.5

Notes:

DoD Directive 5230.24, *Distribution Statements on Technical Documents*, states:

- It is DoD policy to pursue a coordinated and comprehensive program to provide for a strong and viable military research, acquisition, and support program consistent with requirements of national security, export laws, and competitive procurement.



1.6

Notes:

DoD Instruction 3200.14
Principles and Operational Parameters of the DoD Scientific and Technical Information (STI) Program

DoD Policy:

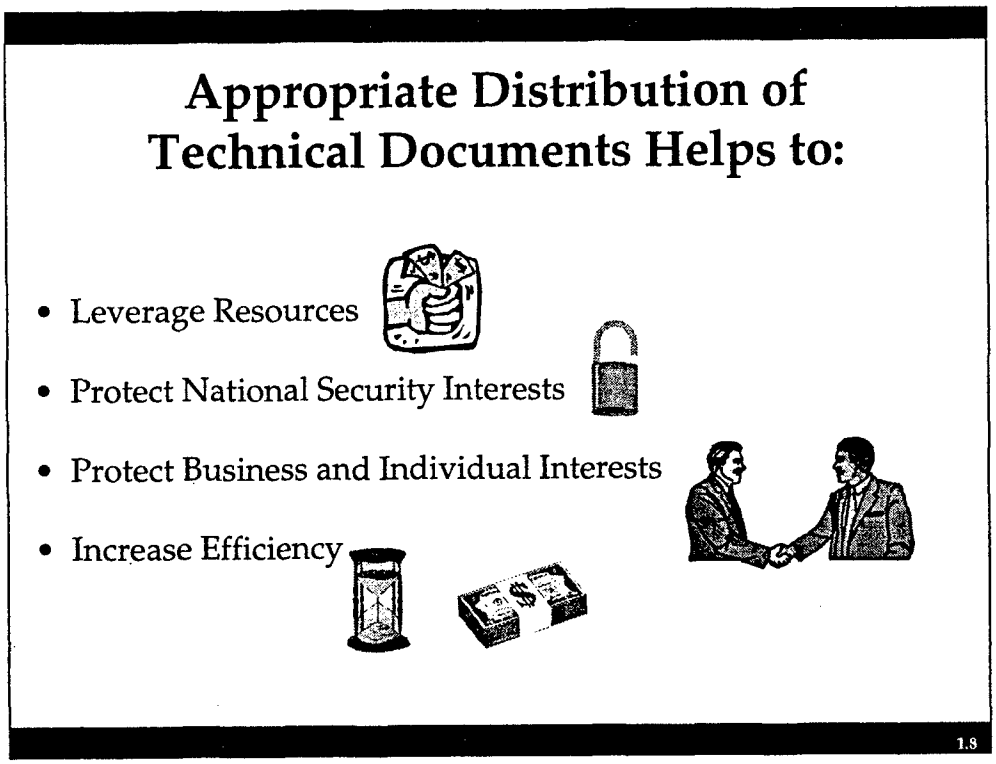
Establish and maintain program to document research and engineering and studies' results.

STI Program:

Support the acquisition, analysis, storage, retrieval, and dissemination of STI.

1.7

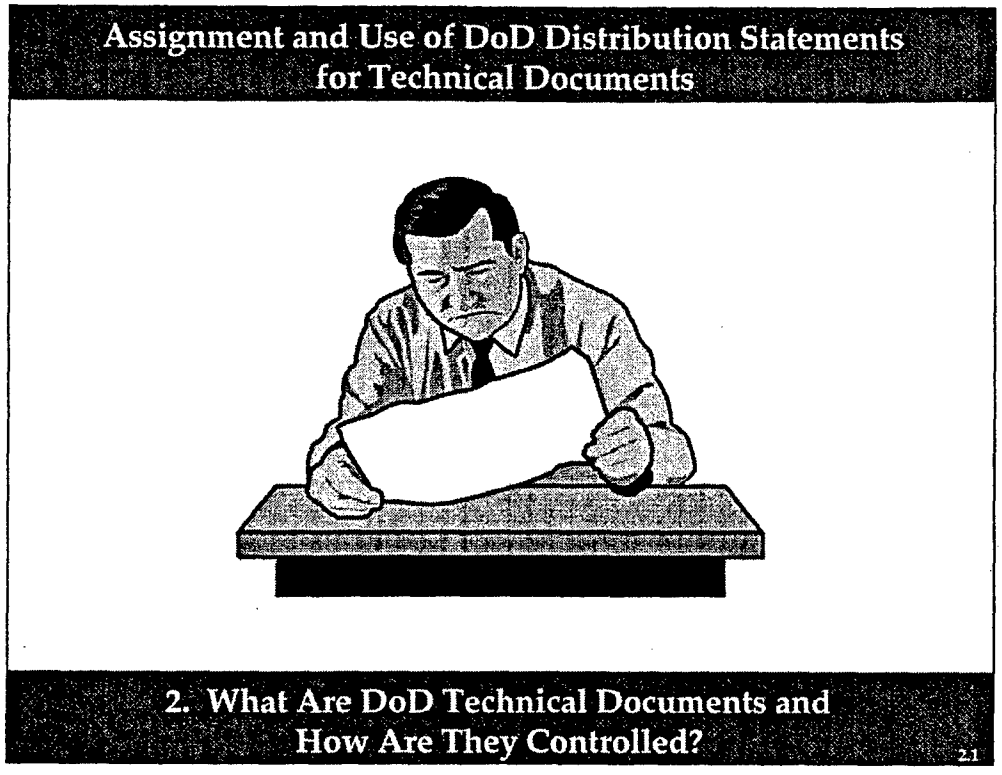
Notes:


Appropriate Distribution of Technical Documents Helps to:
• Leverage Resources
• Protect National Security Interests
• Protect Business and Individual Interests
• Increase Efficiency
1.8

Notes:

Module 2

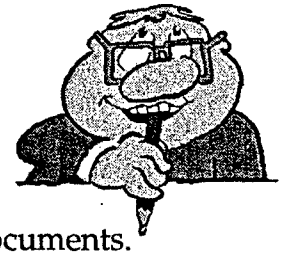
This Page Intentionally Left Blank


Assignment and Use of DoD Distribution Statements for Technical Documents
2. What Are DoD Technical Documents and How Are They Controlled?
2.1

Notes:

Module 2 Objectives

- Distinguish technical documents, data, and information governed by DoD Directive 5230.24, *Distribution Statements on Technical Documents*, from other kinds of information and data.
- Identify the function of DoD Distribution Statements and list their components.
- Understand the relationship of DoDD 5230.24 to other policies that affect the distribution of DoD technical documents.
- Know the formats and media in which technical documents can be found.

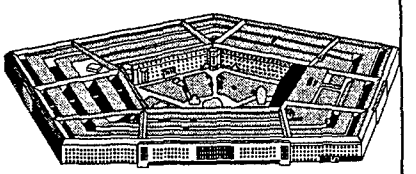


22

Notes:

DoDD 5230.24

- Contains requirements for distribution control of DoD technical documentation
- Applies to:
  - Office of Secretary of Defense
  - Military departments (including National Guard and Reserve Components)
  - Joint Chiefs of Staff
  - Unified and specified commands
  - Defense agencies

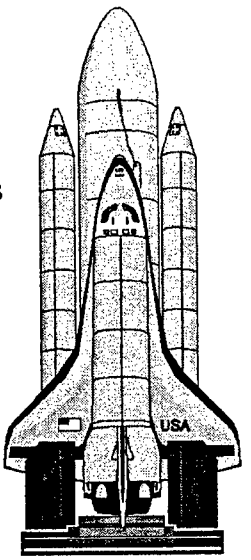


23

Notes:

DoDD 5230.24
Scope

- Newly created DoD technical documents generated by DoD-funded RDT&E programs
- Newly created engineering documents, including software and documentation
- Information about military and space equipment and technology

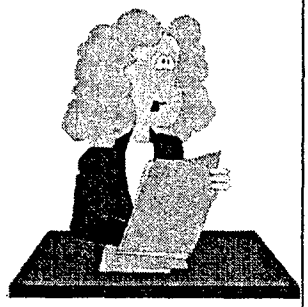


2-1

Notes:

DoDD 5230.24 Requirements

- Responsible DoD components must mark technical documents *before* primary distribution.
- Technical program managers must assign DoD Distribution Statements to control secondary distribution.
- DoD Distribution Statements can only be changed/removed by DoD Controlling Office.

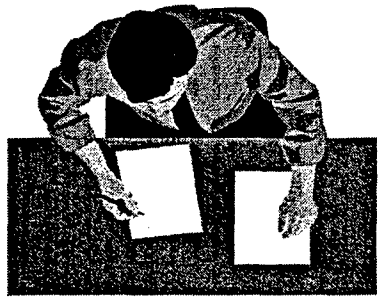


2.5

Notes:

DoDD 5230.24 Requirements, (cont.)

- DoD Controlling Office must establish review procedure.
- DoD Controlling Office must notify DTIC, technical/ engineering centers, and other repositories when changes occur in:
  - address
  - office designation
  - the classification markings, DoDDistribution Statements, or export control statements on its documents



26

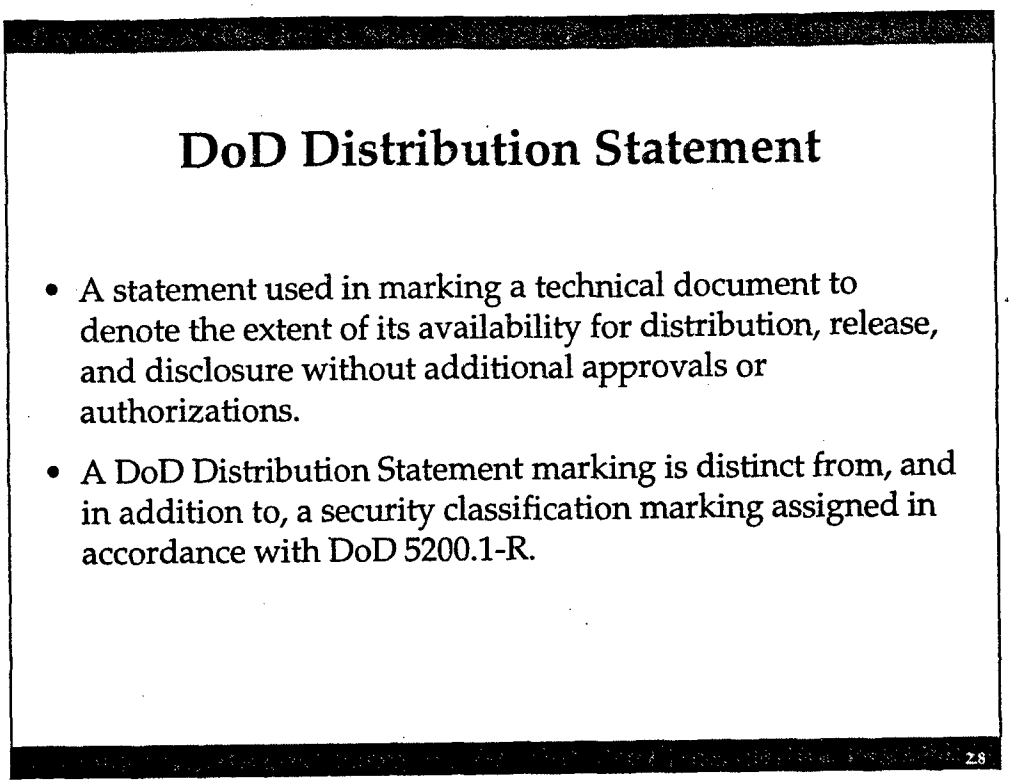
Notes:

Distribution

- **Primary:** the initial targeted distribution of, or access to, technical documents authorized by the DoD Controlling Office
- **Secondary:** release of technical documents provided after primary distribution by other than the originator or DoD Controlling Office; for example, lending, permitting others to read, or releasing the document in whole or part

2.7

Notes:


DoD Distribution Statement
• A statement used in marking a technical document to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations.
• A DoD Distribution Statement marking is distinct from, and in addition to, a security classification marking assigned in accordance with DoD 5200.1-R.
2.8

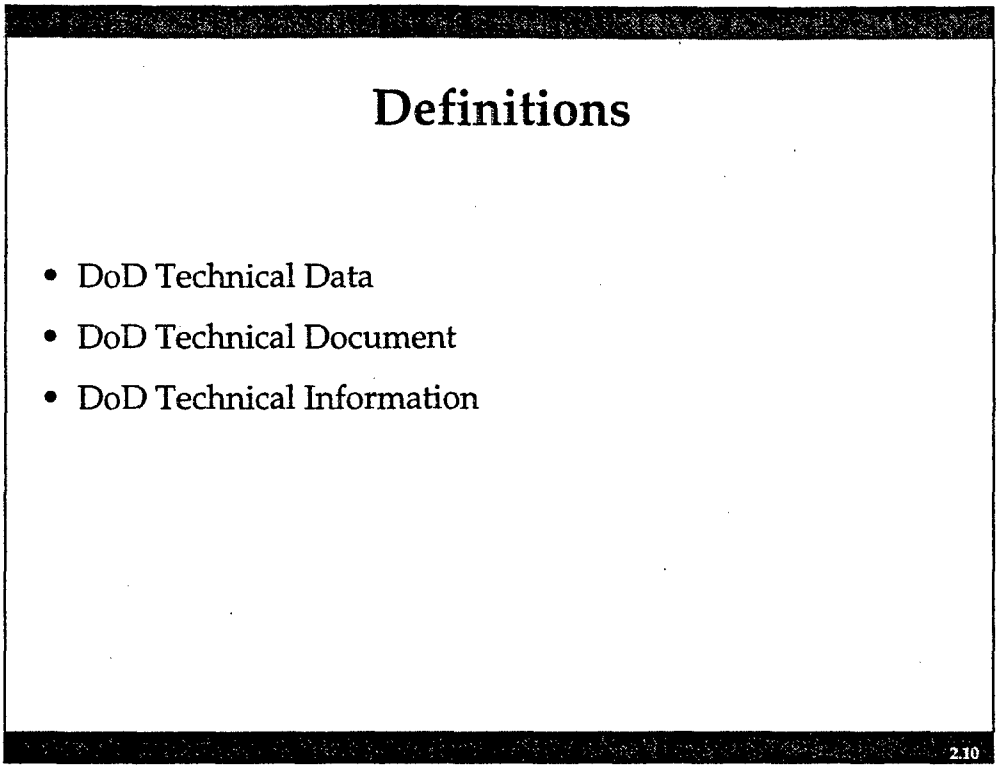
Notes:

Parts of the Distribution Statement

1. Authorized audience
2. Reason for restriction
3. Identity of DoD Controlling Office
4. Date

29

Notes:


Definitions
• DoD Technical Data
• DoD Technical Document
• DoD Technical Information
2.10

Notes:

DoD Technical Data

Recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, support, maintain, operate, repair or overhaul material. The data may be graphic or pictorial delineations in media such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts.

2.11

Notes:

DoD Technical Document

Any recorded information that conveys scientific and technical information or technical data.

Can include:

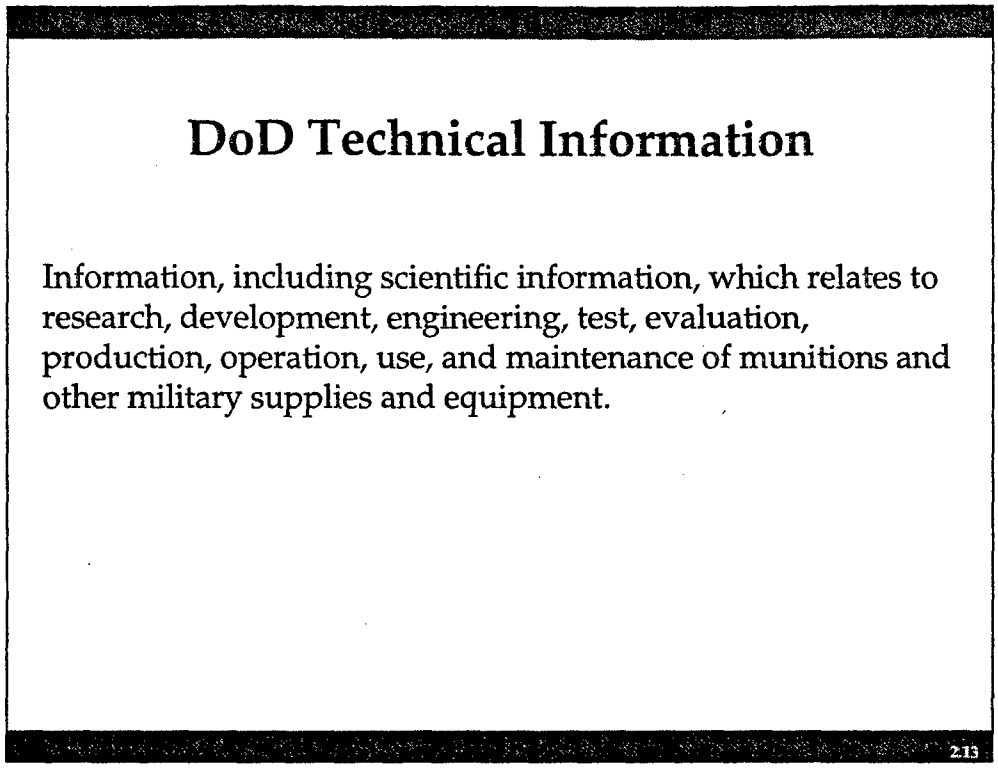
Working papers, memoranda, preliminary reports

Key questions:

Does it have utility beyond immediate mission?
Will it become part of historical record of technical achievements?

2.12

Notes:


DoD Technical Information
Information, including scientific information, which relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment.
2.13

Notes:

Types of DoD Documents

- Studies and Analyses
- Basic Research Planning Documents
- Modernization Planning
- Warfighting Science and Technology Plans
- Defense Technical Area Plans

214

Notes:

Technical Documents That Are Not Governed by DoDD 5230.24

- Technical documents used by DoD, but not produced by or for DoD
- Command, Control, Communication, and Intelligence operational documents
- Communications security documents
- Cryptographic data
- Personnel records
- Administrative papers, internal procedures, catalogs and brochures, monthly status reports, directories, promotional materials, and contract administration documents

2.15

Notes:

Other Programs and Policies Controlling Distribution of Technical Documents

- Security Classification
- Export Control
- Freedom of Information Act (FOIA) Exemptions
- Other Sensitive, Unclassified Markings
- Proprietary and Limited Use Rights

2.16

Notes:

Security Classification Markings

- Protect national security.
- Are authorized by:
  - DoDD 5200.1
  - DoD 5200.1-R
  - DoDD 5220.22
- Are explained in the National Industrial Security Program Operating Manual (NISPOM).
- May control documents after declassification when content remains sensitive.

2.17

Notes:

Export Control

- Data, goods, and technologies found on the State Department's Munitions List and the Department of Commerce Control List must have export control warnings.
- Export-controlled documents cannot be exported without approval, authorization or license.
- Export-controlled documents must have a compatible DoD Distribution Statement.

2.18

Notes:

Freedom of Information Act Exemptions

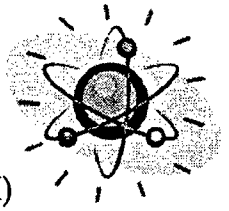
- Unclassified but sensitive material is protected from disclosure by exemptions 2-9 of FOIA:
  - National defense or foreign policy
  - Individual privacy
  - Proprietary business interests
- Not approved for public release
- All distribution statements (except A) are a type of FOUO marking:
  - Provide clear reason for restriction when congruent with FOIA exemptions
  - FOUO marking is not enough on its own!

2.19

Notes:

Other Sensitive, Unclassified Information Markings

- Unclassifed Controlled Nuclear Information (UCNI)
  - Design and security of atomic energy defense facilities
  - declassified nuclear weapons



- Naval Nuclear Propulsion Information (NNPI)
  - nuclear powered ships and nuclear support facilities

2.20

Notes:

Proprietary and Limited Use Rights

The government must control distribution of proprietary data when the owners of that data have:

- designated it proprietary
- granted the government limited rights to its use

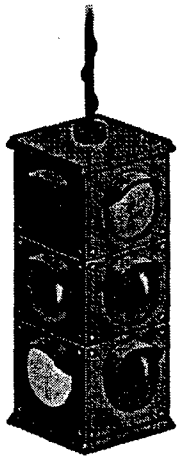
Subpart 27 of DoD supplement to the Federal Acquisition Regulations has detailed information.

2.21

Notes:

DoD Distribution Statements Do's and Don'ts

- **Do** choose a Distribution Statement compatible with other markings/policies.
- **Don't** choose a Distribution Statement that allows the release of documents contrary to the purpose of other policies.



2.22

Notes:

CONFIDENTIAL

SECRET

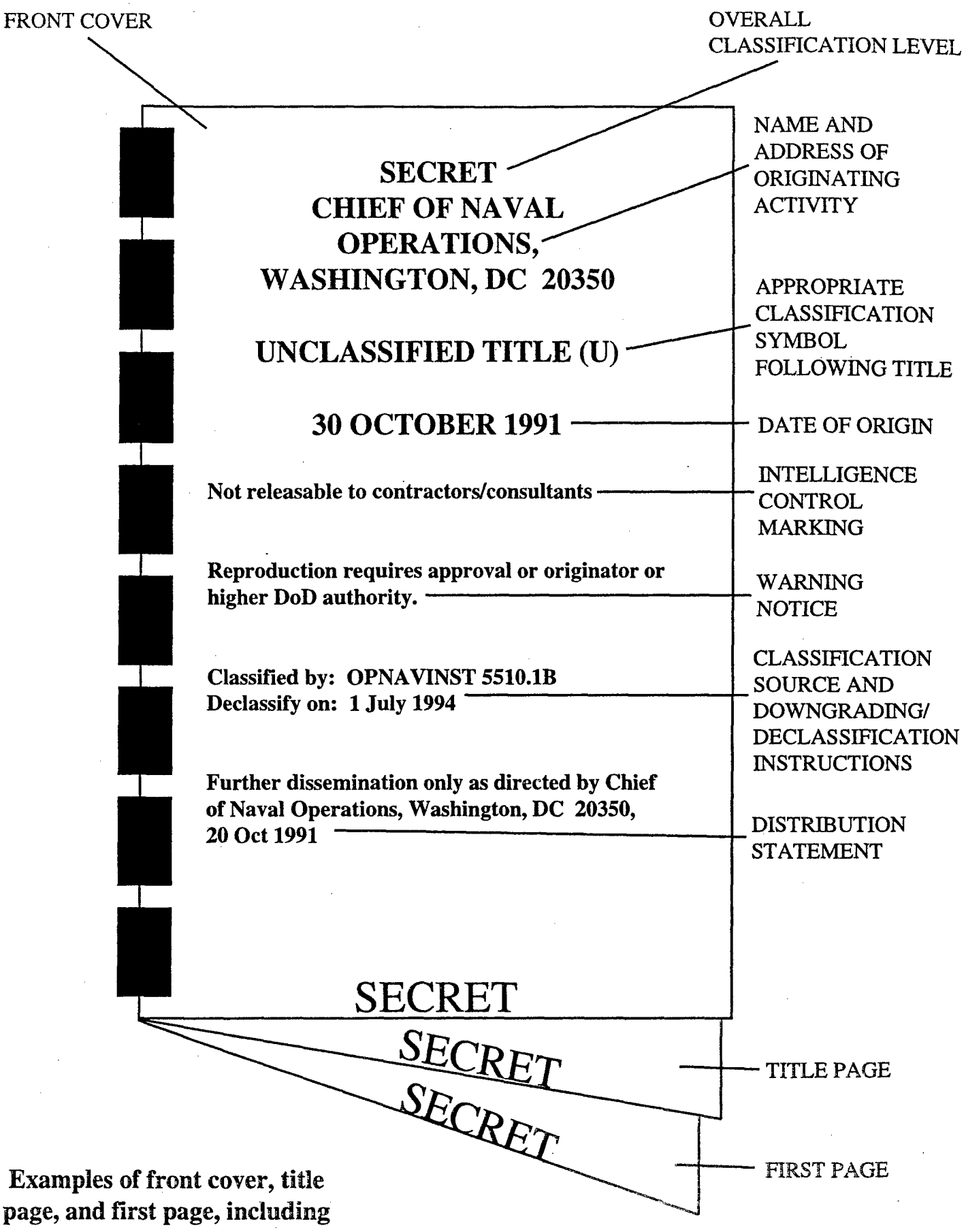
SECRET

CONFIDENTIAL

TOP SECRET

TOP SECRET

Examples of Classification Markings



Examples of front cover, title page, and first page, including warning notices and intelligence control markings, of classified publication.

Office of the Chief
of Naval Operations Washington, DC 20350 October 1991

The Reduction of Reverberation and Ambient Noise by Ocean Surface Films

DESTRUCTION NOTICE - For classified documents, follow the procedures in DoD 5200.22-M, Industrial Security Manual, Section II-19 or DoD 5200.1-R, Information Security Program Regulation, Chapter IX. For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

INSTRUCTIONS FOR COMPLETING DD FORM 2345

PRIVACY ACT STATEMENT

AUTHORITY: U.S. INDIVIDUALS AND ENTERPRISES: 10 USC, section 140c, as added by PL 98-94, Section 1217, September 24, 1983; and implemented by DoDD 5230.25, "Withholding of Unclassified Technical Data From PUBLIC Disclosure," November 8, 1984 (32 CFR Part 250.)

FOR CANADIAN INDIVIDUALS AND ENTERPRISES: Defense Production Act.

PRINCIPAL PURPOSE(S): To identify individuals and enterprises eligible to receive military critical technical data.

ROUTINE USE(S): To support decisions regarding dissemination or withholding of military critical technical data. Information provided on this form describing your business may be published from time to time for the benefit of the "certified contractors."

DISCLOSURE: Voluntary; however, failure to provide the information may result in a denial of access to military critical technical data.

MAIL THE ORIGINAL, COMPLETED COPY OF THIS FORM AND ANY ATTACHMENTS TO:

United States/Canada Joint Certification Office
Defense Logistics Services Center
Federal Center
Battle Creek, Michigan, USA 49017-3084

PRIVACY ACT STATEMENT

1. Mark only one box. Mark "RESUBMISSION" only if your previous submission was returned or rejected. Mark "REVISION" (of a previously accepted submission) to show revised information, such as addresses or business description. Mark "5-YEAR RENEWAL" in response to a renewal notice from U.S./Canada - JCO. When either the "REVISION" or "5-YEAR RENEWAL" box is marked, enter your current Certification Number in Item 7-a.

2. a. For an individual, show full name (Last, First, Middle Initial). For an enterprise, show full name of corporate parent; or institution.

b. Enter the mailing address of the individual or enterprise making the certification. If a P.O. Box is used for mailing purposes, include street address as well.

c. Each corporate subsidiary or division that is to receive military critical technical data must be certified separately. If not applicable, so state.

d. For U.S. Individual or Enterprise, enter the Federal Supply Code for Manufacturers (FSCM) or Non-Manufacturers (FSNCM) or Commercial and Government Entity (CAGE) code assigned to the individual or enterprise making the certification. For a Canadian individual or enterprise, enter the Department of Supply and Services Vendor Code assigned to the individual or enterprise making the certification. If none, so state. If a subsidiary or division is certified, enter the organization's code.

3. Show the name, address, telephone number (including area code) and title of the individual who will receive military critical technical data and be responsible for its further dissemination. A position designation may be used only when conditions described in item 5.a.(1) and (2) are prerequisites for holding that position.

4. Describe the business activity of the entity identified in Item 2 in sufficient detail for the U.S. or Canadian Government agency controlling the data to determine whether the military critical technical data that you may request from time to time are reasonably related to your stated business activity. For example, state that you design and construct high-pressure, high volume hydraulic pumps for use in connection with aircraft control surfaces; do not state simply "hydraulic pumps." Provide concise statements within the space provided.

5. If certifications 5.e. and 5.f. cannot be made, provide (on a separate sheet) a description of any extenuating circumstances that may give sufficient reason to accept your certification.

6. If Item 2 identifies an individual, that individual must sign. If Item 2 identifies an institution or a corporate entity, a person who can legally obligate the enterprise to a contract must sign.

7. Explanation of Certification Action.

a. ACCEPTED. The U.S./Canada -JCO has assigned the individual or enterprise identified in Item 2.a., a Certification Number which will identify the individual or enterprise as a "certified contractor" as defined in U.S. DoDD 5230.25 or Canada's TDCR. The acceptance is valid for a period of five years from the acceptance date unless sooner revoked under the provisions of U.S. DoDD 5230.25 or Canada's TDCR. If at any time a certified contractor is unable to adhere to the conditions under which a certification was accepted, the contractor's certification is considered void, and the contractor will either submit a revised certification or surrender all military critical technical data obtained under this agreement to the data controlling offices specified on the documents.

b. RETURNED. Your submission did not contain all the information required to process your certification. Pleas review any comments provided with the returned submission and resubmit in accordance with the applicable instructions.

c. REJECTED. Reasons for rejection include, for example, debatement, a business activity that does not fall within the scope of U.S. DoDD 5230.25 or Canada's TDCR, or failure to make all of the required certifications.

LEGEND:

DoD = Department of Defense
DoDD = Department of Defense Directive
U.S./Canada -JCO = United States/Canada Joint Certification Office
DSS = Department of Supply and Services
TDCR = Technical Data Control Regulations
Military Critical Technical Data = Unclassified technical data as governed by U.S. DoDD 5230.25 or Canada's TDCR.

PRIVACY ACT STATEMENT

Section 8911 of Title 5 to the U.S. Code authorizes collection of this information. The primary use of this information is by management and your payroll office to approve and record your use of leave. Additional disclosures of the Information may be: To the Department of Labor when processing a claim for compensation regarding a job connected injury or illness; to a State unemployment office regarding a claim; to Federal Life Insurance or Health Benefits carriers regarding a claim; to a Federal, State, or local law enforcement agency where your agency becomes aware of a violation or possible violation of civil or criminal law; to a Federal agency when conducting an investigation on you for employment or security reasons; to the Office of Personnel Management or General Accounting Office when the information is required for evaluation of leave administration; and to the General Services Administration in connection with its responsibilities for records management.

Where the employee identification number is your Social Security Number, collection of this information is authorized by Executive Order 9397. Furnishing the information on this form, including your Social Security Number, is voluntary, but failure to do so may result in disapproval of this request.

If your agency uses the information furnished on this form for purposes other than those indicated above, it may provide you with an additional statement reflecting these purposes.

TECHNICAL VOLUME: Distribution Statement D

Distribution authorized to DoD and U.S. DoD contractors only; Reason: administrative/operational use; July 21, 1998. Other requests for this document shall be referred to AFRL/HEOP.

Additional distribution is also authorized to the Canadian Department of Defence and Canadian DND contractors in accordance with the provisions of a Foreign Military Sales agreement between this organization and the Canadian Department of Defence.

COST VOLUME: Distribution Statement E

Distribution authorized to DoD Components only; Reason: Proprietary information; July 21, 1998. Other requests for this document shall be referred to AFRL/HEOP.

Additional distribution is also authorized to the Canadian Department of Defence in accordance with the full knowledge and written consent of the companies that provided the proprietary (sensitive cost) information provided by them to the U.S. Government.

Example of DoD Distribution Statement with an Approved Exception

PARTICIPANT ACTIVITY: 10 minutes

What Do You Know About Technical Documents, Data, and Information?

The following True/False Quiz is an exercise to see how much you already know about what is meant by "technical documents, data, and information." It is *not* a test. Please take a few minutes to read the statements, and then circle T for "True" or F for "False." Your instructor will go over the answers when everyone is finished.

True/False Quiz

Which of the following should be considered technical documents, data, or information?

T F The base map for Aberdeen Proving Ground.

T F An e-mail message detailing the delays in the shipment of construction materials which are responsible for the delays in the construction of a new hangar for the Stealth bomber at Whiteman Air Force Base.

T F An e-mail message detailing problems with the fabrication of a new wing design for the Stealth bomber at Whiteman Air Force Base.

T F The Navy System Manager's Guide to the Source Data System, which contains software code for system management and configuration for the Navy payroll and personnel management system.

T F The Navy Disbursing Clerk's End User Guide for the Source Data System's payroll function, containing directions for entering pay data.

T F A contractor's monthly status report on research being conducted on occurrence of diseases related to service in the Gulf War, which contains statistical research data from field units.

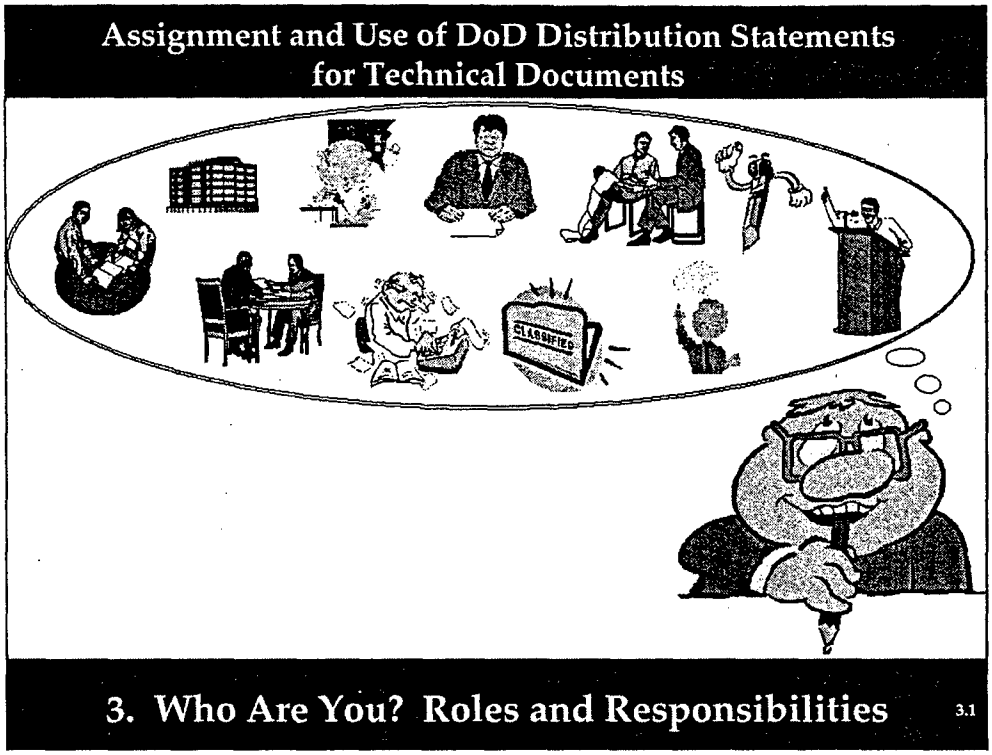
T F A contractor's monthly status report on research being conducted on occurrence of diseases related to service in the Gulf War, which details timelines and funds expended.

Scientific and technical information can come in the following forms:

T	F	Audio taped dictation	T	F	Oral Presentation
T	F	ASCII code	T	F	Photographs
T	F	Informal memos	T	F	Engineering Drawings
T	F	HTML documents	T	F	Computer Floppy Disks
T	F	Internal project meeting minutes	T	F	Microfilm

Module 3

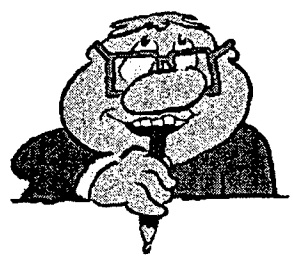
This Page Intentionally Left Blank


Assignment and Use of DoD Distribution Statements
for Technical Documents
3. Who Are You? Roles and Responsibilities
3.1

Notes:

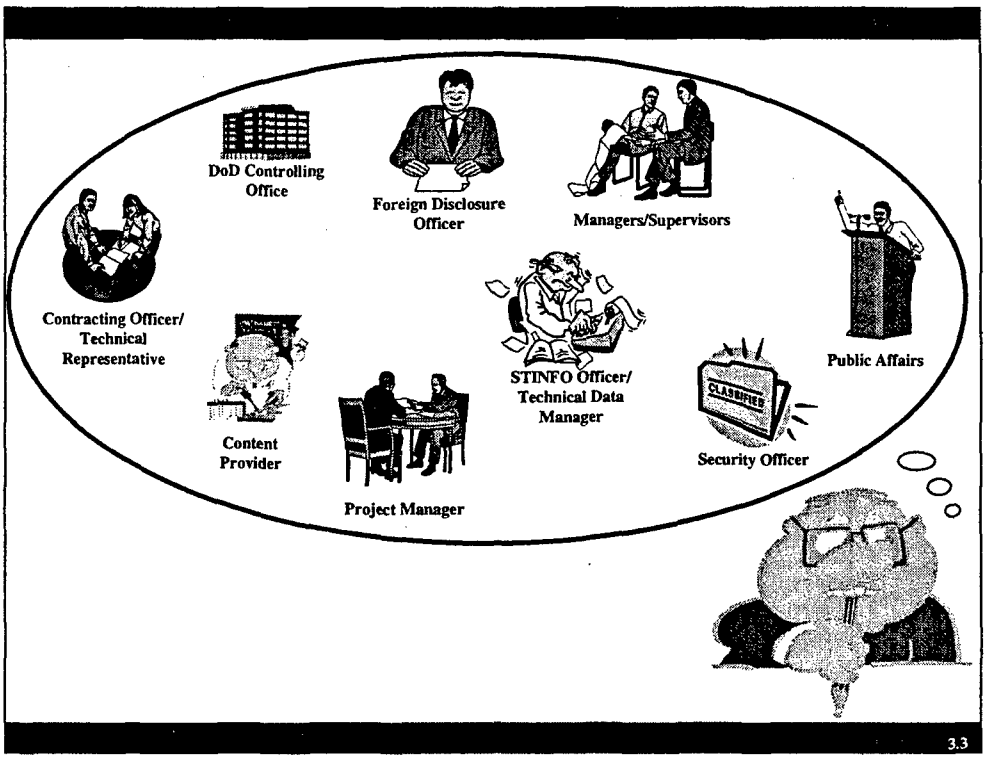
Module 3 Objective

- The participant will be able to identify the roles and responsibilities associated with marking of DoD technical documents, information, and data with Distribution Statements.



3.2

Notes:

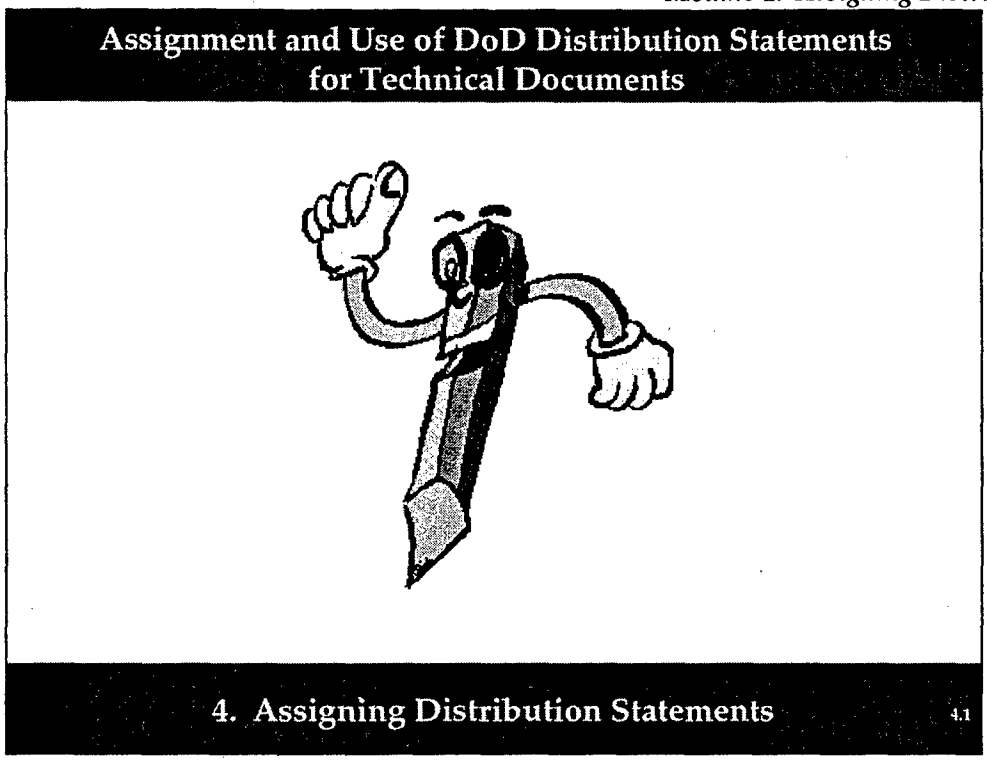

DoD Controlling Office
Foreign Disclosure Officer
Managers/Supervisors
Contracting Officer/ Technical Representative
Public Affairs
STINFO Officer/ Technical Data Manager
CLASSIFIED
Content Provider
Security Officer
Project Manager
3.3

Notes:

This Page Intentionally Left Blank

Module 4

This Page Intentionally Left Blank

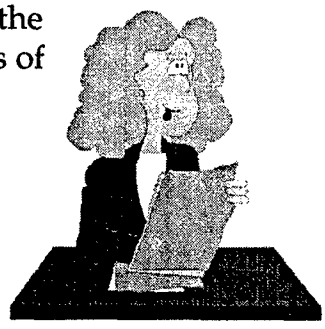

Assignment and Use of DoD Distribution Statements
for Technical Documents
4. Assigning Distribution Statements
4.1

Notes:

Module 4 Objective

Using the job aids provided, the participant will be able to:

- demonstrate the process for correctly assigning DoD Distribution Statements to technical documents
- place DoD Distribution Statements in the appropriate location on different types of media

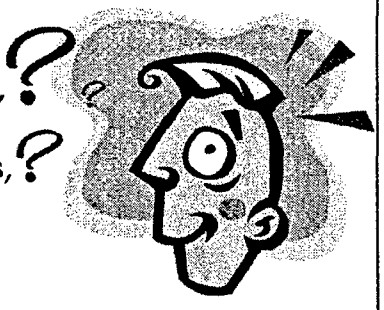


4.2

Notes:

Questions to Answer

- How do I select the most appropriate DoD Distribution Statement?
- Where does the DoD Distribution Statement go on printed documents, magnetic data, microfiche, drawings, photographs, viewgraphs, oral presentations, and audiovisual productions?



4.3

Notes:

Steps

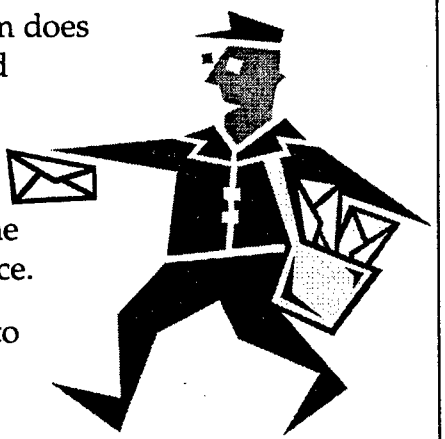
1. **Technical Content**: Is the content technical in nature?
   - YES? Go to question 2.
   - NO? Then no need to mark.
2. **DoD Technical Document**: Was it produced by or for DoD?
   - YES? Then DoD Directive 5230.24 applies. You must mark it. Go to question 3.
   - NO? Then no need to mark.

4.4

Notes:

Steps (cont.)

3. **Primary Distribution**: To whom does the DoD Controlling Office need to send it? This is the "primary distribution" for the document.



- It should be congruent with the secondary distribution audience.
- Don't send copies out yet; go to Step 4 first!

4.5

Notes:

Steps (cont.)

4. **Secondary Distribution**: Who do you think can or cannot receive this technical content without further review or release decision by the DoD Controlling Office?
   - To answer this question, use:
     - Your knowledge of the project
     - Relevant information about the content
     - Any supporting documents
     - Expertise of other DoD staff
   - Use the matrix of "Reasons for Designating Audiences" to select appropriate audiences for the technical content.

4.6

Notes:

Steps (cont.)

Step 4 (cont.)

- Work your way through all the questions:
  - YES to any question?
  - Consider the need to restrict your document's secondary distribution to one of the audience defined in the matrix. The outcome of your decision will be the choice of one of
  - six distribution levels B, C, D, E, F, or X
  - NO to all questions?
  - If the document does not contain sensitive the information
  - and if the Public Affairs Office concurs, the document
  - should be approved for release to the general public and
  - assigned DoD Distribution Statement A.

47

Notes:

Steps (cont.)

5. **DoD Distribution Statement:** Assign the Distribution Statement, providing all needed information and placing it correctly on the materials.

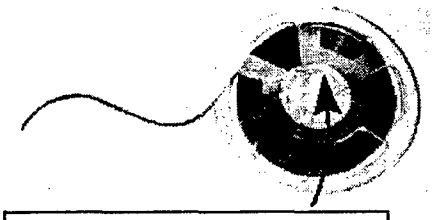
6. **Review and Concurrence:** Check your decision with:
   - your own management
   - Public Affairs
   - Security and Foreign Disclosure Officers
   - your STINFO Officer or Technical Data Manager

4.8

Notes:

Placing the Distribution Statement

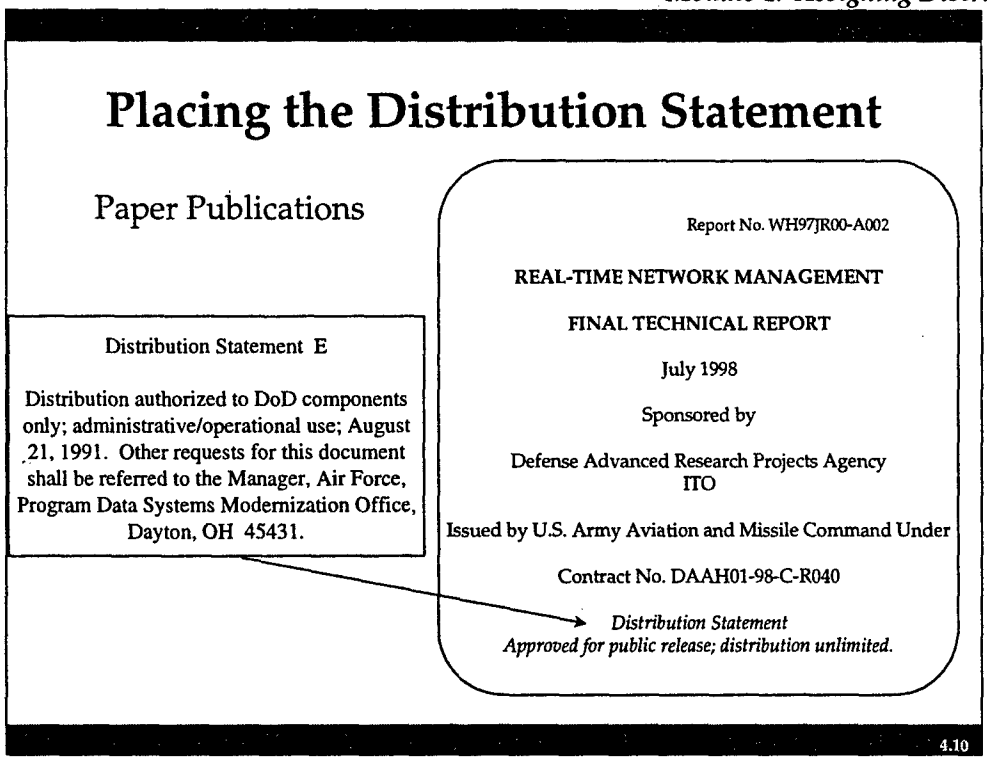
- Correct placement varies with the format or media.
- For any format or media, any required export control notices must be placed along with the distribution statement.



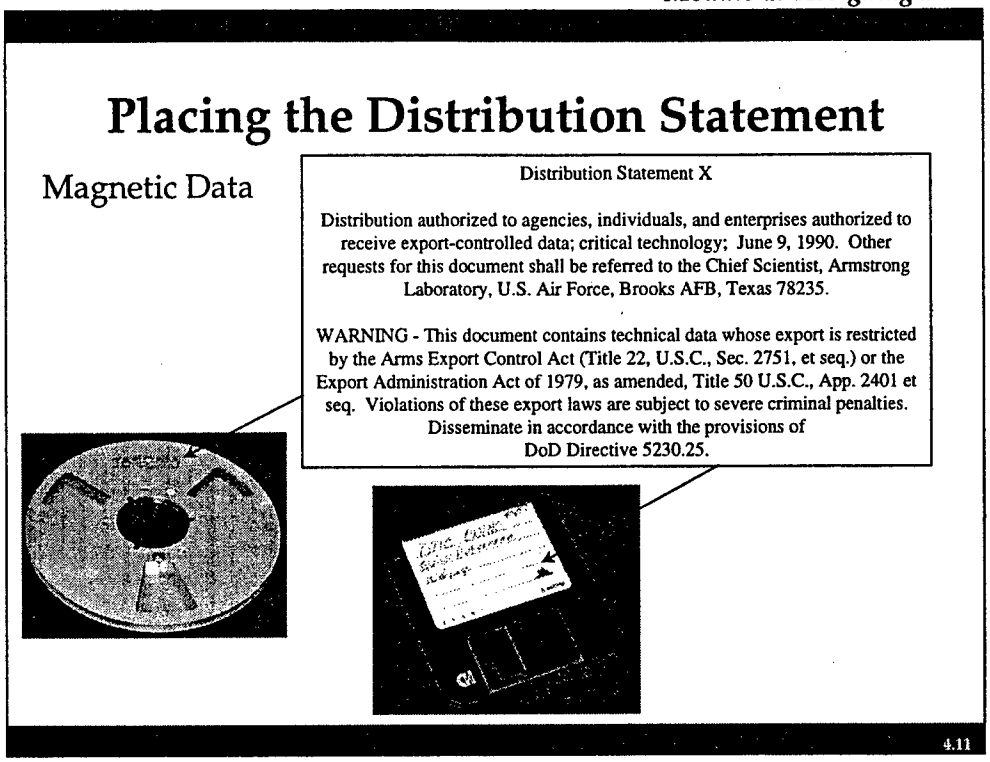
Distribution Statement F
Further dissemination only as directed by the
Chief of Naval Research,
Arlington, VA 22217,
May 14, 1997.

4.9

Notes:


Placing the Distribution Statement
Paper Publications
Distribution Statement E
Distribution authorized to DoD components only; administrative/operational use; August 21, 1991. Other requests for this document shall be referred to the Manager, Air Force, Program Data Systems Modernization Office, Dayton, OH 45431.
Report No. WH97JR00-A002
REAL-TIME NETWORK MANAGEMENT
FINAL TECHNICAL REPORT
July 1998
Sponsored by
Defense Advanced Research Projects Agency
ITO
Issued by U.S. Army Aviation and Missile Command Under
Contract No. DAAH01-98-C-R040
Distribution Statement
Approved for public release; distribution unlimited.
4.10

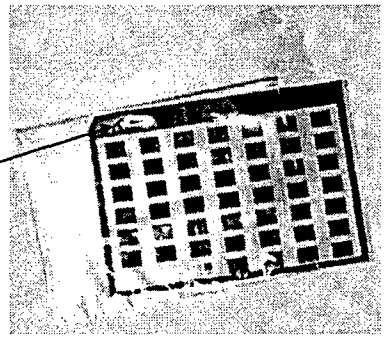
Notes:


Placing the Distribution Statement
Magnetic Data
Distribution Statement X
Distribution authorized to agencies, individuals, and enterprises authorized to receive export-controlled data; critical technology; June 9, 1990. Other requests for this document shall be referred to the Chief Scientist, Armstrong Laboratory, U.S. Air Force, Brooks AFB, Texas 78235.
WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec. 2751, et seq.) or the Export Administration Act of 1979, as amended, Title 50 U.S.C., App. 2401 et seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with the provisions of DoD Directive 5230.25.
4.11

Notes:

Placing the Distribution Statement

Microfiche



Distribution Statement B

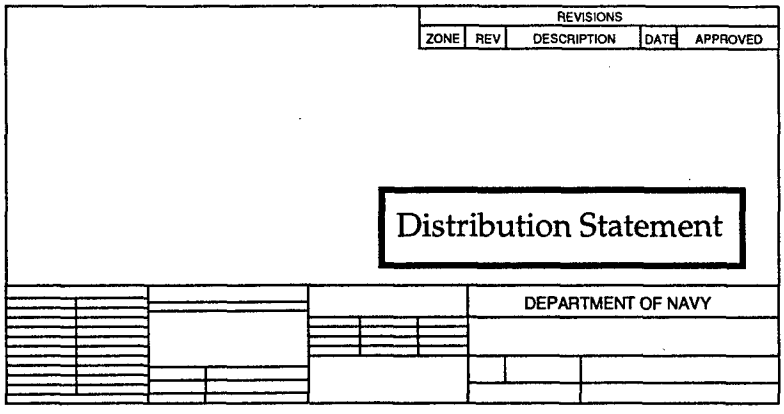
Distribution authorized to U.S. Government Agencies only; foreign government information; September 15, 1995. Other requests for this document shall be referred to the Naval Sea Logistics Center, Naval Sea Systems, Concord, CA 94510.

4.12

Notes:

Placing the Distribution Statement

Drawings

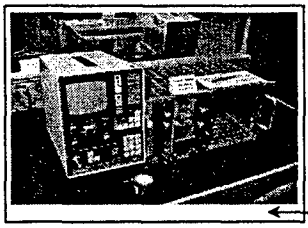


4.13

Notes:

Placing the Distribution Statement

Photographs



Distribution Statement D

Distribution authorized to DoD components and their contractors only; administrative/operational use; February 6, 1997. Other requests for this document shall be referred to the Commander, U.S. Army Test and Evaluation Command, Aberdeen Proving Ground, MD 21005.

(Back of Photo)

4.14

Notes:

Placing the Distribution Statement

Presentation Viewgraphs/Slides

Distribution Statement E

Distribution authorized to DoD components only; direct military support; July 1, 1996. Other requests for this document shall be referred to the Director, Sensor Technology Office, Defense Advanced Research Projects Agency, Arlington, VA 22203.

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 of 1979, as amended, Title 50 U.S.C., App. 2401 et. seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

Presentation Title

Distribution Statement E

Distribution authorized to DoD components only; direct military support; July 1, 1996. Other requests for this document shall be referred to the Director, Sensor Technology Office, Defense Advanced Research Projects Agency, Arlington, VA 22203.

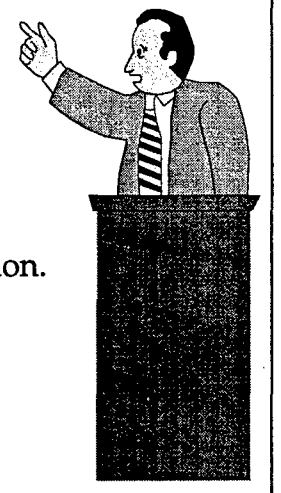
Presentation Slide

4.15

Notes:

Placing the Distribution Statement

Oral Presentations



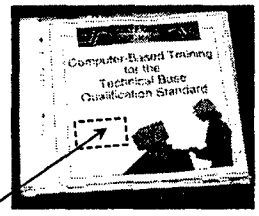
Verbally state the applicable DoD Distribution Statement and export control requirement at the beginning of the presentation.

4.16

Notes:

Placing the Distribution Statement

Audio-Visual Productions



Distribution Statement E

Distribution authorized to DoD components only; critical technology; October 1991. Other requests shall be referred to the Chief of Naval Operations, Washington, DC 20350.

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 of 1979, as amended, Title 50 U.S.C., App. 2401 et. seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

APRIL 18, 1991
CNO
Washington, DC 20350

4.17

Notes:

This Page Intentionally Left Blank

References

This Page Intentionally Left Blank

DoDD 3200.12

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 3200.12

February 11, 1998

DDR&E

SUBJECT: DoD Scientific and Technical Information (STI) Program (STIP)

References: (a) DoD Directive 3200.12, "DoD Scientific and Technical Information Program," February 15, 1983 (hereby canceled)
(b) Title 10, Section 133, United States Code
(c) DoD Instruction, 3200.14, "Principles and Operational Parameters of the DoD Scientific and Technical Information Program" May 13, 1997
(d) DoD 5025.1-M, "DoD Directives System Procedures," August 1994, authorized by DoD Directive 5025.1, June 24, 1994
(e) through (t), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update DoD policy and responsibilities consistent with the general authority of the Secretary of Defense under reference (b) for establishing the DoD STIP.

1.2. Authorizes the issuance of reference (c), consistent with reference (d), to provide guidance on implementation of policies and principles for the DoD STIP.

1.3. Authorizes the issuance of DoD Instruction 3204.1 (reference (e)), consistent with reference (d), to provide implementation of policy and principles for the DoD Industry Independent Research and Development Program.

1.4. Authorizes the issuance of DoD 3200.12-R-4 (reference (f)), consistent with reference (d) to provide guidance for the implementation of policy and principles for

the DoD Domestic Technology Transfer Program.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). The term "Military Services," as used herein, refers to the Army, the Navy, the Air Force, and the Marine Corps.

2.2. Does not apply to the following:

2.2.1. DoD programs for involving day-to-day operational data used by the warfighter unless required for scientific and technical analysis and communications and display of information relating to the command and control of operations and forces.

2.2.2. The DoD scientific and technical intelligence production community and those products generated under that program, and technical documents containing classified scientific and technical intelligence (although the concepts and principles of the DoD STIP shall be applied when possible).

2.2.3. The DoD technical data management program, (DoD 5000-2-R, reference (g)) for those aspects that are distinct from STI.

2.2.4. Signal intelligence and communications security information, as defined in DoD Directives S-3115.7 and C-5200.5 (references (h) and (i)).

3. DEFINITIONS

OSD Principal Staff Assistants (PSAs). The Under Secretaries of Defense, the Director of Defense Research and Engineering, the Assistant Secretaries of Defense, the Director of Operational Test and Evaluation, the General Counsel of the Department of Defense, the Inspector General of the Department of Defense, the Assistants to the Secretary of Defense, and the OSD Directors or equivalents who report to the Secretary or Deputy Secretary of Defense.

4. POLICY

It is DoD policy that:

4.1. The Department of Defense shall aggressively pursue a coordinated and comprehensive STIP, thereby providing maximum contribution to the advancement of science and technology. The STIP shall permit timely, effective, and efficient conduct and management of DoD research and engineering (R&E) and studies programs, and eliminate unnecessary duplication of effort and resources by encouraging and expediting the interchange and use of STI. Interchange and use of DoD STI is intended to include the DoD Components, their contractors, other Federal Agencies, their contractors, and the national and international R&E community. Acquisition, documentation, and dissemination of STI is further described in DoD Instructions 3200.14, 3204.1, and DoD 3200.12-R-4 (references (c), (e), and (f)), and is controlled in a manner consistent with references (j) through (r).

4.2. The STIP is a basic and integral part of the functions of the organization of the Under Secretary of Defense for Acquisition and Technology (USD(A&T)) (DoD Directive 5134.1, reference (s)), the functions of the Director of Defense Research and Engineering (DoD Directive 5134.3, reference (t)), and is affected by the DoD studies program. Managers and performers of R&E shall use and support the STIP. STI services and processes are used to facilitate communication and enrich development and use of STI during the planning and conduct of R&E and studies efforts. Conversely, the performance of those R&E and studies efforts is not considered complete until the STI, including related program management information, is documented satisfactorily and provided to the applicable STI distribution activities.

4.3. Defense R&E programs consist of several critical elements necessary to meet the technological needs of the Department of Defense in support of the DoD national security mission. The DoD Components shall coordinate, sustain, and integrate those critical R&E elements described in paragraphs 4.3.1. through 4.3.3., below, and in a manner designed to maximize the ability to meet DoD mission requirements. These elements are:

4.3.1. Critical facilities in the public and private sector needed to produce world class technology;

4.3.2. Highly skilled and experienced people in Department of Defense and defense-related academic and industrial complexes that produce and apply the

technology needed to sustain DoD technological superiority; and

4.3.3. A well-established and sustained DoD STIP at all levels to record, disseminate, and preserve as a critical asset the investment in and results of the other two elements of the DoD R&E programs. While STI is often unobtrusive or taken for granted when it is well-managed, failure to support adequately the STIP materially impacts DoD ability to leverage significant investments in defense technology.

5. RESPONSIBILITIES

5.1. Under Secretary of Defense for Acquisition and Technology shall:

5.1.1. Manage the STIP.

5.1.2. Issue DoD Instructions 3200.14 and 3204.1, and DoD 3200.12-R-4 (references (c), (e), and (f)).

5.2. The OSD Principal Staff Assistants shall ensure that STIP matters in their respective areas are consistent with the policy in Section 4., above, and references (c), (e), and (f).

5.3. The Heads of the DoD Components shall implement this Directive and the policy and principles in references (c), (e), and (f). That includes the responsibility to:

5.3.1. Designate a "senior-level STI director or manager" at the Military Department or Defense Agency staff level who shall serve as a single, authoritative point of contact for management and oversight of STIP matters.

5.3.2. Continually review their needs for STI and make proposals to the Office of the Under Secretary of Defense for Acquisition and Technology (OUSD (A&T)) for the initiation of new or major revisions to STI efforts or activities.

5.3.3. Establish, operate, and administer those STI functions and activities required for the conduct of their missions, and other information activities required to serve the Department of Defense, national R&D needs, or as assigned by the OUSD (A&T).

5.3.4. Provide programming, budgeting, funding, and other fiscal support for their STI activities.

6. EFFECTIVE DATE

This Directive is effective immediately.

John J. Hamre
Deputy Secretary of Defense

Enclosures - 1
1. References

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 3204.1, "Independent Research and Development," December 1, 1983

(f) DoD 3200.12-R-4, "Domestic Technology Transfer Program Regulation," December 1988, authorized by this Directive

(g) DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs," March 1996, authorized by DoD Directive 5000.1, March 15, 1996

(h) DoD Directive S-3115.7, "Signals Intelligence (SIGINT) (U)," January 25, 1973

(i) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990

(j) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(k) DoD 5200.1-R, "Department of Defense Information Security Program Regulation," January 1997, authorized by DoD Directive 5200.1, December 13, 1996

(l) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988

(m) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

(n) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996

(o) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

(p) DoD Directive 2002.3, "Clearance of Research and Studies with Foreign Affairs Implications," August 15, 1985

(q) DoD Directive 5230.25, "Withholding Unclassified Technical Data from Public Disclosure," November 6, 1984

(r) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987

(s) DoD Directive 5134.1, "Under Secretary of Defense for Acquisition and Technology (USD(A&T))," June 8, 1994

(t) DoD Directive 5134.3, "Director of Defense Research and Engineering (DDR&E)," August 31, 1994

DoDD 5220.22

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 5220.22

December 8, 1980

USD(P)

SUBJECT: DoD Industrial Security Program

References: (a) DoD Directive 5220.22, subject as above, December 1, 1976 (hereby canceled)
(b) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended by Executive Order 10909, January 17, 1961
(c) DoD Directive 5025.1, "Department of Defense Directives System," October 16, 1980
(d) DoD Directive 5220.6, "Industrial Personnel Security Clearance Program," December 20, 1976
(e) DoD Directive 5122.5, "Assistant Secretary of Defense (Public Affairs)," July 10, 1961

1. REISSUANCE AND PURPOSE

1.1. This Directive reissues reference (a) to implement reference (b) within the Department of Defense; assigns overall responsibility for policy and administration of the Defense Industrial Security Program (DISP); and ensures that classified information released to industry is properly safeguarded.

1.2. This Directive authorizes the following publications to be issued in accordance with the provisions of reference (c):

1.2.1. The Industrial Security Regulation (DoD 5220.22-R). This document prescribes detailed policies and procedures applicable to all user agencies in carrying out their responsibilities under the DISP.

1.2.2. The Industrial Security Manual for Safeguarding Classified

Information (DoD 5220.22-M) and supplements thereto. This document is incorporated by reference into the Department of Defense Security Agreement and is part of the basic contract between the Government and those contractors who require access to classified information.

1.2.2.1. The document also is incorporated by reference into each contract, the performance of which requires access to classified information by the contractor or his or her employees.

1.2.2.2. DoD 5220.22-M prescribes the specific requirements, restrictions, and other safeguards considered necessary in the interest of national security for the safeguarding of classified information.

1.2.3. The Industrial Security Letter. This document, which is issued as needed, provides guidance for industry in carrying out its responsibilities under the DISP.

1.2.4. Industrial Security Bulletin. This document, which is issued as needed, provides guidance to those in Government having responsibilities related to the administration of the DISP.

2. APPLICABILITY

The provisions of this Directive apply to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, and the Defense Agencies (hereafter referred to as "DoD Components").

3. POLICY

3.1. As provided in E.O. 10865 (reference (b)), the Secretary of Defense is authorized to prescribe, by regulation, such specific requirements, restrictions, and other safeguards as are considered necessary to protect:

3.1.1. Classified information provided to or within U.S. industry that relates to the bidding on, negotiation, award, performance, or termination of contracts with DoD Components.

3.1.2. Other classified information provided to or within industry that the Department of Defense has responsibility for safeguarding.

3.2. For the purposes of this Directive, U.S. industry includes any industrial, educational, commercial, or other entity and shall be referred to as "industry".

3.3. In addition, the Secretary of Defense is authorized to enter into agreements with any other Department or Agency of the Executive Branch to extend the regulations he prescribes to safeguard classified information provided to industry by these Departments or Agencies (4.1.6., below). Such other Departments and Agencies, as well as DoD Components, shall be referred to in this Directive as "user Agencies."

3.4. The Department of Defense shall set forth policies, practices, and procedures to be followed by user Agencies for the effective protection of classified information provided to industry, including foreign classified information the U.S. Government is obliged to protect in the interest of national security.

3.5. DoD Directive 5220.6 (reference (d)) established the standard and criteria for making security clearance determinations when persons employed in private industry require access to classified information.

3.6. DoD Directive 5122.5 (reference (e)) established the responsibility of the Assistant Secretary of Defense (Public Affairs) for the review of information pertaining to classified contracts before public disclosures by DoD contractors.

4. RESPONSIBILITIES

4.1. The Deputy Under Secretary of Defense (Policy Review) (DUSD(PR)) shall:

4.1.1. Be responsible for overall policy guidance and management oversight of the DISP.

4.1.2. Approve the issuance of changes to DoD 5220.22-M and DoD 5220.22-R.

4.1.3. Develop policies, plans, and programs for the DISP, and approve changes before issuance by the Director, Defense Investigative Service (DIS).

4.1.4. Coordinate with other offices in the OSD, as appropriate, all proposed policies, plans, and programs before referral for issuance by the Director, DIS.

4.1.5. Determine the effectiveness of the operation and administration of the

DISP.

4.1.6. Upon request of other Government Departments or Agencies, under E.O. 10865 (reference (b)), arrange, on behalf of the Department of Defense, to apply the provisions of the DISP to contractors of such Departments or Agencies, and render industrial security services required for the safeguarding of classified information released by such Departments or Agencies to industry. The Director, DIS, shall be kept currently informed of such agreements.

4.2. The Assistant Secretary of Defense (Public Affairs), unless otherwise delegated, shall review and clear information pertaining to classified contracts before public disclosures by DoD contractors. Contractors shall be required, as a contract obligation, to submit information materials described above according to DoD 5220.22-M.

4.3. The Director, Defense Investigative Service, under the general supervision of the General Counsel, DoD, shall administer the DISP as a separate program element on behalf of all DoD Components. In this capacity, the Director, DIS, shall assume security cognizance for all contractors and industrial facilities under the DISP on behalf of the Department of Defense, DoD Components, and user Agencies, and shall provide investigative support, as required, for the administration of the DISP. In addition, the Director, DIS, shall:

4.3.1. Develop appropriate changes to maintain DoD 5220.22-R and DoD 5220.22-M, including supplements thereto, on a current and effective basis. Proposed changes to these documents shall be forwarded to the ODUSD(PR), ATTN: Director, Security Plans and Programs, for preliminary policy review.

4.3.2. Refer proposed changes to DoD 5220.22-R and DoD 5220.22-M to the DUSD(PR), ATTN: Director, Security Plans and Programs and publish changes expeditiously, upon approval by the DUSD(PR).

4.3.3. Prepare, coordinate and publish the Industrial Security Letter and Bulletin on approval by the DUSD(PR), ATTN: Director, Security Plans and Programs.

4.3.4. Present on an annual basis, the James S. Cogswell Award to selected contractors in recognition of sustaining a superior security program for safeguarding classified information.

4.3.5. Budget, fund, and administer the DISP, including the appropriate field

extensions. (The Defense Logistics Agency shall make appropriate funds available to DIS through FY 81.)

4.4. The Heads of DoD Components shall ensure that all their contracts requiring contractor access to classified information come within the purview of the DISP.

4.5. The Secretaries of the Military Departments shall provide counter-intelligence support when requested.

5. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective October 1, 1980. Forward two copies of implementing documents to the Deputy Under Secretary of Defense (Policy Review) within 120 days.

W. Graham Claytor, Jr.
Deputy Secretary of Defense

This Page Intentionally Left Blank

DoDD 5230.9

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 5230.9

April 9, 1996

Administrative Reissuance Incorporating Change 1, July 15, 1999

WHS

SUBJECT: Clearance of DoD Information for Public Release

References: (a) DoD Directive 5230.9, subject as above, April 2, 1982 (hereby canceled)

(b) *DoD Directive 5110.4, "Washington Headquarters Services (WHS)," May 10, 1999*

(c) DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978

(d) DoD Directive 5220.22, "DoD Industrial Security Congress," December 8, 1980

(e) through (u), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policy and responsibilities for the security and policy review and clearance of official DoD information proposed for official public release by the Department of Defense and its employees under reference (b).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, *the* Combatant Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.1.2. All DoD employees.

2.2. For provisions governing review of:

2.2.1. Prepared statements, transcripts of testimony, and other material provided to congressional committees that may be included in the published records, reference (c) applies.

2.2.2. Information before publication or disclosure by DoD contractors, DoD Directive 5220.22 and DoD 5220.22-M (references (d) and (e)) apply.

2.2.3. Release of official information in litigation, DoD Directive 5405.2 (reference (f)) applies.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Accurate and timely information is made available to the public, the Congress, and the news media to help the analysis and understanding of defense strategy and national security issues.

4.2. Any official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense shall be reviewed for clearance by appropriate security review and public affairs offices prior to release.

4.3. The public release of official DoD information is limited only as necessary to safeguard information requiring protection in the interest of national security or other legitimate governmental interest, as authorized by references (g) through (t).

4.4. Information released officially is consistent with established national and DoD policies and programs.

4.5. The Inspector General of the Department of Defense, as an independent and

objective office in the Department of Defense, is exempt from the policy review provisions of this Directive. As necessary, information may be submitted for security review prior to public release.

4.6. To ensure a climate of academic freedom and to encourage intellectual expression, students (including midshipmen and cadets) and faculty members (DoD civilian or military) of an academy, college, university or DoD school are not required to submit for review papers or materials that are prepared in response to academic requirements and not intended for release outside the academic institution. Information that is intended for public release or made available in libraries to which the public has access shall be submitted for review. Clearance shall be granted if classified information is not disclosed, the DoD interests in nonclassified areas are not jeopardized, and the author accurately portrays official policy, even if the author takes issue with that policy.

4.7. Retired personnel, former DoD employees, and nonactive duty members of the Reserve components may use the review services to ensure that the information intended for public release does not compromise national security.

4.8. DoD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DoD forums or media. Such activity is authorized if:

4.8.1. No laws or regulations are violated.

4.8.2. Ethical standards and compliance with DoD Directive 5500.7 and DoD 5500.7-R (references (q) and (r)) are maintained.

4.8.3. The preparation activities are not done during normal duty hours or with the use of DoD facilities, property, or personnel except as authorized by references (q) and (r).

4.8.4. The author does not use official DoD information generally not available to the public and which would not be released under DoD 5400.7-R (reference (m)).

5. RESPONSIBILITIES

5.1. The *Director, Washington Headquarters Services,* shall:

5.1.1. Monitor compliance with this Directive.

5.1.2. Develop procedures and review guidelines for the security and policy review of information intended for public release in coordination with offices of OSD Principal Staff Assistants.

5.2. The Heads of the DoD Components shall:

5.2.1. Provide prompt guidance and assistance to the *Director, Washington Headquarters Services (WHS),* when requested, for the security or policy implications of information proposed for public release.

5.2.2. Establish policies and procedures to implement this Directive in their Components.

5.2.3. Forward official DoD information proposed for public release that is determined to require clearance by the *Director, WHS,* to the *Director, Freedom of Information and Security Review,* for review, including recommendation on the releasability of the information being forwarded.

6. EFFECTIVE DATE

This Directive is effective immediately.

John P. White
Deputy Secretary of Defense

Enclosures - 2
1. References, continued
2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995, authorized by DoD Directive 5220.22, December 8, 1980

(f) DoD Directive 5405.2, "Release of Official Information in Litigation and Testimony of DoD Personnel as Witnesses," July 23, 1985

(g) DoD Directive 5200.1, "DoD Information Security Program," *December 13, 1996*

(h) DoD 5200.1-R, "Information Security Program Regulation," *January 1997*, authorized by DoD Directive 5200.1, *December 13, 1996*

(i) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(j) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

(k) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987

(l) DoD Directive 5400.7, "DoD Freedom of Information Act Program," *September 29, 1997*

(m) DoD 5400.7-R, "DoD Freedom of Information Act Program," *September 1998*, authorized by DoD Directive 5400.7, *September 29, 1997*

(n) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

(o) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983, authorized by DoD Directive 5400.11, June 9, 1982

(p) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983

(q) DoD Directive 5500.7, "Standards of Conduct," August 30, 1993

(r) DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993, authorized by DoD Directive 5500.7, August 30, 1993

(s) International Traffic in Arms Regulations (ITAR), Department of State, November 1989

(t) Executive Order 12958, "Classified National Security Information," April 20, 1995

(u) Title 10, United States Code

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. DoD Employee

E2.1.1.1. Any DoD civilian officer or employee (including special Government employees) of any DoD Component (including any nonappropriated fund activity).

E2.1.1.2. Any active duty Regular or Reserve military officer, warrant officer, and active duty enlisted member of the Army, Navy, Air Force, or Marine Corps.

E2.1.1.3. Any Reserve or National Guard member on active duty under orders issued pursuant to 10 U.S.C. (reference (u)).

E2.1.1.4. Any Reserve or National Guard member performing official duties, including while on inactive duty for training or while earning retirement points, pursuant to reference (u), or while engaged in any activity related to the performance of a Federal duty or function.

E2.1.1.5. Any faculty member in a civil service position or hired pursuant to reference (u), and any student (including a cadet or midshipman) of an academy, college, university, or school of the Department of Defense.

E2.1.1.6. Consistent with labor agreements and international treaties and agreements, and host country laws, any foreign national working for a DoD Component except those hired pursuant to a defense contract.

E2.1.2. Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form.

E2.1.3. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department.

DoDI 5230.29

This Page Intentionally Left Blank

Department of Defense

INSTRUCTION

NUMBER 5230.29

August 6, 1999

WHS

SUBJECT: Security and Policy Review of DoD Information for Public Release

References: (a) DoD Instruction 5230.29, same subject as above, May 6, 1996 (hereby canceled)
(b) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
(c) DoD Directive 5400.4, "Provision of Information to Congress," January 30, 1978
(d) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987
(e) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984
(f) International Traffic in Arms Regulation (ITAR), Department of State, November 1989

1. PURPOSE

This Instruction:

1.1. Reissues reference (a).

1.2. Implements policy, assigns responsibilities, identifies information that must be cleared before public release, and prescribes procedures under reference (b) to carry out security and policy review of DoD information for public release.

2. APPLICABILITY

This Instruction applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the

Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

3. DEFINITIONS

Terms used in this Instruction are defined in enclosure 2 of reference (b).

4. POLICY

It is DoD policy under reference (b) that a security and policy review shall be done on all official DoD information intended for public release that pertains to military matters, national security issues, or subjects of significant concern to the Department of Defense.

5. RESPONSIBILITIES

5.1. The Director, Washington Headquarters Services shall:

5.1.1. Monitor compliance with the procedures established in section 6., below, for the security and policy review of official DoD information.

5.1.2. Provide for the prompt security and policy review of official DoD information proposed for public release that is originated by, in, or for the Department of Defense, to include statements intended for open presentation before the Congress and other material submitted to the Congress in accordance with DoD Directive 5400.4 (reference (c)). The review is made to ensure that properly classified information is not disclosed and no conflict exists with established policies or programs of the Department of Defense or the U.S. Government.

5.1.3. Coordinate, as necessary, with the staffs of the DoD Components when reviewing official DoD information for public release clearance to ensure accuracy and currency of existing policy and security guidance.

5.1.4. Respond to requests for review of information submitted voluntarily by non-DoD sources or DoD personnel acting in a private capacity to ensure that such material does not contain classified information. This review shall also address technology transfer and public releasability of technical data under DoD Directives 5230.24 and 5230.25, and the ITAR (references (d) through (f)).

5.2. The General Counsel of the Department of Defense shall conduct legal reviews, as needed, to ensure compliance with applicable laws and regulations to protect DoD rights and interests.

5.3. The Heads of the DoD Components shall:

5.3.1. Ensure compliance with this Instruction and issue any guidance necessary for the internal administration of the requirements prescribed in section 6., below.

5.3.2. Forward official DoD information specified under subsection 6.1., below, which is proposed for public release to the Director, Washington Headquarters Services, ATTN: Director for Freedom of Information and Security Review (DFOISR), for review and clearance, as prescribed in subsection 6.2., below, with specific recommendation on the releasability of the information being forwarded.

5.3.3. Provide prompt guidance and assistance to the Director, WHS, when requested, on any information proposed for public release.

5.3.4. Exercise clearance authority for information not specified under subsection 6.1., below. This authority may be delegated to the lowest level competent to evaluate the content and implications of public release of the information.

6. PROCEDURES

6.1. Clearance Requirements. Official DoD information that is prepared by or for DoD personnel and is proposed for public release shall be submitted to the Director, WHS, ATTN: DFOISR, 1400 Defense Pentagon, Room 2C757, Washington, DC 20301-1155, for review and clearance, if the information:

6.1.1. Originates or is proposed for release in the Washington, DC area;

6.1.2. Is or has the potential to become an item of national or international interest;

6.1.3. Affects national security policy or foreign relations;

6.1.4. Concerns a subject of potential controversy among the DoD Components or with other Federal Agencies;

6.1.5. Is presented by a DoD employee, who by virtue of rank, position, or expertise would be considered an official DoD spokesperson;

6.1.6. Contains technical data, including data developed under contract or independently developed and controlled by the ITAR (reference (f)) that may be militarily critical and subject to limited distribution, but on which a distribution determination has not been made; or,

6.1.7. Bears on any of the following subjects:

6.1.7.1. New weapons or weapons systems, or significant modifications or improvements to existing weapons or weapons systems, equipment, or techniques.

6.1.7.2. Military operations, significant exercises, and operations security.

6.1.7.3. National Command Authorities; command, control, communications, computers, and intelligence; information operations and computer security.

6.1.7.4. Military activities or application in space; nuclear weapons, including nuclear weapons effects research; chemical warfare and defensive biological warfare; and arms control treaty implementation.

6.1.7.5. Any other contemporary topic that is designated by the Head of a DoD Component.

6.2. Submission for Review. The following procedures apply to all information required to be submitted to DFOISR for clearance:

6.2.1. A minimum of three copies of material, in its final form, shall be submitted, together with DD Form 1910, "Clearance Request for Public Release of Department of Defense Information," to DFOISR.

6.2.2. Any material submitted for review shall be initialed by the speaker, author, or other authorized individual acting for the principal to indicate approval of the text.

6.2.3. All information submitted for review to DFOISR must first be coordinated within the originating DoD Component to ensure that it reflects the

organization's policy position and does not contain classified information requiring withholding.

6.2.4. Only the full and final text of material proposed for release shall be submitted for review. Notes, outlines, briefing charts, etc., may not be submitted as a substitute for a complete text.

6.2.5. Abstracts to be published in advance of a complete paper, manuscript, etc., require clearance. Clearance of an abstract does not fulfill the requirement to submit the full text for clearance before its publication. If an abstract is cleared in advance, that fact, and the DFOISR case number assigned to the abstract, shall be noted on the DD Form 1910 or other transmittal when the full text is submitted.

6.2.6. The requirements of DoD Directive 5400.4 (reference (c)) shall apply to the processing of information proposed for submission to Congress.

6.2.7. Information intended for placement on electronic bulletin boards accessible through the INTERNET, or other publicly accessible computer servers, requires review and clearance for public release if, it meets the requirements of subsection 6.1., above.

6.3. Time Limits

6.3.1. Submit speeches and briefings a minimum of 3 working days before the event. Additional time may be needed for complex or potentially controversial speeches.

6.3.2. Papers, articles, and other material shall be submitted a minimum of 5 working days before the date needed. The length, complexity, and content shall determine the number of reviewing Agencies and, consequently, the time required for the complete review process.

6.3.3. Technical papers shall require a minimum of 10 working days. The majority of papers are processed in that time-frame. Occasionally, more time is needed if the material is complex or requires review by several Agencies.

6.4. Effect of Review Actions and Appeals

6.4.1. Information reviewed for public release clearance shall result in one of the following actions:

6.4.1.1. Cleared for Open Publication. The information may be released without restriction by the originating Component or its authorized official. DFOISR may require a disclaimer to accompany the information, as follows:

"The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government."

6.4.1.2. Cleared "as amended" for open publication. Amendments, made in red, are binding on the submitter. Red brackets identify information that must be deleted. When possible, alternative wording is provided to substitute for the deleted material. Occasionally, wording will be included that shall be added to the text before public release. A disclaimer, as in subparagraph 6.4.1.1., above, may also be required."

6.4.1.2. Not Cleared. The information submitted for review may not be released.

6.4.2. Although DFOISR has no responsibility for correcting errors of fact or making editorial changes, obvious errors may be identified in the text and noted as "recommended." Those corrections are not binding on the author or submitter.

6.4.3. All amendments or "not cleared" determinations may be appealed through DFOISR to the Director, WHS. All appeals shall be resolved at the lowest practical level and as quickly as possible.

7. EFFECTIVE DATE

This Instruction is effective immediately.

D. O. Cooke, Director
Washington Headquarters Services

DoDD 5230.11

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 5230.11

June 16, 1992

USD(P)

SUBJECT: Disclosure of Classified Military Information to Foreign Governments and International Organizations

References: (a) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," December 31, 1984 (hereby canceled)

(b) DoD Instruction 5230.17, "Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations," February 17, 1985 (hereby canceled)

(c) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (short title: National Disclosure Policy (NDP-1)), October 1, 1988[1]

(d) through (t), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a), replaces reference (b), implements reference (c), and updates policy, responsibilities, and procedures governing proposed disclosures of classified military information to foreign governments and international organizations (hereafter referred to as "foreign governments").

---

1 Provided to designated disclosure authorities on a need-to-know basis from the Office of the Director for International Security Programs, Office of the Deputy Under Secretary of Defense for Security Policy (ODUSD(SP)).

2. APPLICABILITY AND SCOPE

This Directive applies to:

2.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. All disclosures of classified military information defined in enclosure 2 Disclosures of military intelligence information, however, also must be in compliance with DoD Directive C-5230.23 (reference (d)).

2.3. Classified information involved in munitions license applications processed under DoD Directive 2040.2 and the ITAR (references (e) and (f)).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2

4. POLICY

It is U.S. national and DoD policy under NDP-1 (reference (c)) that:

4.1. Classified military information is a national security asset that shall be protected and shall be shared with foreign governments only when there is a clearly defined benefit to the United States. Disclosures of such information shall be made only when authorized by officials designated under this Directive and then only when all requirements of this Directive are met.

4.2. An official who has been specifically delegated disclosure authority under section 5., below, may authorize disclosures of classified military information to foreign governments in support of a lawful and authorized U.S. Government purpose if the:

4.2.1. Official represents the DoD Component that originated the information.

4.2.2. Level of classified information to be disclosed does not exceed the classification level delegated by Annex A of reference (c).

4.2.3. Criteria and conditions in enclosure 3 are satisfied.

4.3. The Secretary of Defense and the Deputy Secretary of Defense are the only DoD officials who have original authority to grant exceptions to the policy contained in this Directive. The Secretary of Defense has delegated authority to the National Military Information Disclosure Policy Committee (NDPC) to consider and grant requests for exceptions to policy in compliance with reference (c).

4.4. Classified military information shall not be disclosed to foreign nationals until the appropriate designated disclosure authority receives a security assurance from the recipient foreign government on the individuals who are to receive the information.

4.5. In accordance with reference (c), it is U.S. policy to avoid creating false impressions of U.S. readiness to make available classified military information, materiel, or technology. Accordingly, designated disclosure authorities of the originating DoD Component, or, when an exception to policy is required, the Secretary of Defense, the Deputy Secretary of Defense or the NDPC must authorize, in advance, proposals to be made to foreign governments that could lead to the eventual disclosure of classified military materiel, technology, or information. Commitments shall not be expressed or implied, and no disclosures shall be made pending the required disclosure decision.

4.6. Disclosure planning shall include the following:

4.6.1. Planning for possible foreign involvement should start at the beginning of the weapon system acquisition process and other programs, to facilitate decisions on the disclosure of classified and controlled unclassified information in support of cooperative programs, foreign participation in the DoD procurement activities, and foreign sales. The planning shall include consideration of the requirements set forth in DoD Instruction 5000.2, Part 5, Section F (reference (g)).

4.6.2. The DoD Components shall use the Technology Assessment/Control Plan in DoD Directive 5530.3 (reference (h)) as the basis for making the stated disclosure decisions in paragraph 4.6.1., above, on weapon system programs.

4.6.3. A delegation of disclosure authority lefter (DDL) similar to that in enclosure 4 shall be used to provide disclosure guidance to subordinate commands and Agencies and, when applicable, to the DoD contractors.

4.7. All disclosures and denials of classified military information shall be

reported in the Foreign Disclosure and Technical Information System (FORDTIS), in accordance with DoD Instruction 5230.18 (reference (i)). For denials, disclosure authorities must take special care to record a concise summary of the analysis that led to the denial.

4.8. Under conditions of actual or imminent hostilities, any Unified or Specified Commander may disclose classified military information through TOP SECRET to an actively participating allied force when support of combined combat operations requires the disclosure of that information. The appropriate U.S. Commander shall notify the Chairman of the Joint Chiefs of Staff of such disclosures. The Chairman of the Joint Chiefs of Staff, in turn, shall notify the Office of the Under Secretary of Defense for Policy, ATTN: Chairman, NDPC, who shall determine any limitations that should be imposed on continuing disclosure of the information. The U.S. Commander shall be informed of any limitations through the Chairman of the Joint Chiefs of Staff.

4.9. The classified military information that is approved for foreign disclosure shall be transmitted to the intended foreign recipient through government-to-government channels, in accordance with DoD 5200.1-R, chapter 8 (reference (j)).

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Policy shall:

5.1.1. Ensure effective implementation of the National Disclosure Policy and operation of the NDPC under NDP-1 (reference (c)).

5.1.2. Designate the Chair of the NDPC, who shall represent the Secretary of Defense on the NDPC.

5.1.3. Advise the DoD Components and the NDPC about security matters on disclosures.

5.1.4. Draft and negotiate with foreign governments, in coordination with the other applicable DoD Components and Federal Departments and Agencies, security agreements governing the safeguarding of classified military information and equipment.

5.1.5. Coordinate on all international agreements negotiated under DoD

Directive 5530.3 (reference (h)) that involve the disclosure of classified military information.

5.1.6. Review and approve, when justified, requests for disclosure authority from heads of the OSD organizational elements and the DoD Components not covered in subsection 5.2., below.

5.1.7. Issue policy governing international visits, the assignment of liaison officers and exchange officers, and other assignments of foreign representatives to the DoD Components and defense contractors.

5.1.8. Maintain effective liaison with security officials of allied and friendly governments with which the U.S. Government has entered into security agreements.

5.1.9. Direct, manage, and control the FORDTIS, in accordance with DoD Instruction 5230.18 (reference (i)).

5.1.10. Issue necessary supplemental publications for the effective implementation of this Directive.

5.1.11. Publish an annual schedule to keep the DoD Components informed of security survey support requirements.

5.1.12. Record decisions rendered on requests for exception to reference (c) in the FORDTIS, in accordance with reference (i).

5.2. The Under Secretary of Defense for Policy, in addition to the responsibilities in subsection 5.1., above, and the Secretaries of the Military Departments, the Under Secretary of Defense (Acquisition), the Chairman of the Joint Chiefs of Staff, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), the Director, Defense Intelligence Agency, and the Director, National Security Agency/Central Security Service, shall:

5.2.1. Authorize disclosures or denials of the U.S. classified military information for which they are the originating DoD Component in accordance with this Directive.

5.2.2. Designate a senior official to be the principal disclosure authority for their DoD Component. Such designations shall be in writing, with a copy provided to the Chair of the NDPC.

5.2.3. Provide disclosure authority, in writing, to the heads of commands and Agencies and major staff elements under their direction, control, or authority, as necessary, to ensure efficient operation of those commands, Agencies, and staff elements.

5.2.4. Require that the heads of commands, Agencies, and staff elements to whom disclosure authority has been provided appoint a designated disclosure authority.

5.2.5. Coordinate with the Chair of the NDPC all proposed disclosure decisions to be referred directly to the Secretary of Defense or the Deputy Secretary of Defense.

5.2.6. Provide the necessary support to the Chair of the NDPC to do security surveys of foreign government security programs. (See subparagraph 6.9.3.2., below.)

5.2.7. Forward any inquiries concerning this Directive to the Office of the Under Secretary of Defense for Policy, Attn: Deputy Under Secretary of Defense (Security Policy).

5.2.8. Ensure that the principal disclosure authorities shall:

5.2.8.1. Control disclosures for their respective DoD Component.

5.2.8.2. Ensure the competency of subordinate officials appointed as designated disclosure authorities.

5.2.8.3. Ensure that all proposed disclosure actions originating in their DoD Component are coordinated with the other DoD Components that have a joint or shared interest in the information involved.

5.2.8.4. Designate a member and an alternate to represent their DoD Component on the NDPC and ensure that the persons designated:

5.2.8.4.1. Are thoroughly familiar with the daily administration of disclosure activities in their respective DoD Component.

5.2.8.4.2. Are qualified to provide broad professional guidance on matters brought before the NDPC.

5.2.8.4.3. Have direct access to the DoD Component's principal

disclosure authority as well as to other members of the NDPC.

5.2.8.5. Ensure that their DoD Component's disclosure decisions are reported to the FORDTIS in accordance with DoD Instruction 5230.18 (reference (i)).

5.2.8.6. Coordinate requests for disclosures of classified military information involved in litigation with the General Counsel of the Department of Defense or the General Counsel of the DoD Component concerned, as appropriate, before determining whether to disclose the requested information.

5.2.8.7. Ensure that Component personnel traveling overseas are provided disclosure guidance and are informed of and comply with the policy for overseas travel described in DoD 5200.1-R, chapter 8 (reference (j)).

5.3. The Chairman of the Joint Chiefs of Staff shall represent the Commanders of the Unified and Specified Commands on the NDPC.

5.4. The General Counsel of the Department of Defense shall:

5.4.1. Ensure the legal adequacy of security agreements between the United States and foreign governments that establish procedures for the protection of the classified military information.

5.4.2. Advise the DoD Components and the NDPC on the legal aspects of applying the NDP-1 (reference (c)) to individual disclosure decisions.

5.5. The Assistant to the Secretary of Defense (Atomic Energy) shall inform the other NDPC members on the current implementation of international agreements made under the Atomic Energy Act (reference (k)). That includes any statutory determinations and requirements placed on recipient foreign governments and international organizations for safeguarding atomic information released to them.

5.6. The Secretary of the Air Force shall provide resources for the operation, maintenance, and administration of the FORDTIS, and comply with DoD 7110.1-M (reference (l)) on requests for funds to carry out that FORDTIS responsibility.

6. PROCEDURES

6.1. International Agreements

6.1.1. Early Disclosure Determination. Before any discussions with foreign representatives on the negotiation of an international agreement that is governed by DoD Directive 5530.3 (reference (h)), the DoD Components shall determine the extent to which classified military information will be required for release, and obtain disclosure authorization for the information. (See subsection 4.6., above.)

6.1.2. Security Requirements. International agreements that involve the disclosure of classified military information shall contain, at a minimum, the security requirements in section E3.1.2. of enclosure 3. If a general security agreement exists with the foreign government concerned, this requirement may be satisfied by referencing that agreement. Such agreements shall be coordinated with the Office of the Under Secretary of Defense for Policy, ATTN: Deputy Under Secretary of Defense (Security Policy), who may specify other requirements during coordination.

6.1.3. Cooperative Programs. Disclosure authorities shall review carefully any request for classified military information made in accordance with a cooperative agreement with both the goals of the program and the interests of national security in mind.

6.2. Meetings, Symposia, and Conferences. The conduct and organization of meetings, symposia, and conferences where classified military information is to be disclosed shall be in accordance with DoD Directive 5200.12 and DoD 5200.1-R (references (m) and (j)).

6.2.1. Foreign Participation. Foreign nationals may participate in such gatherings when their participation is in accordance with this Directive and U.S. export control policies, the appropriate designated disclosure authorities have approved any classified or controlled unclassified information for disclosure to the proposed foreign attendees, the foreign attendees actively participate in the proceedings, and there is reciprocity for the U.S. Government and industry representatives.

6.2.2. Disclosure Levels. The classification levels and categories of information authorized for disclosure vary among nations. The DoD Components shall limit the level of classified information to be disclosed at meetings attended by foreign representatives to the lowest level that is common to all nations represented.

6.3. Foreign Visitors, Liaison Officers, and Exchange Personnel. Procedures on such individuals shall be in accordance with DoD Directive 5230.20 (reference (n)). Disclosures of classified information shall be in accordance with this Directive.

6.4. Sales, Leases, Loans, or Grants of Classified Items. In implementing the policy in subsection 4.5., above, the DoD Components shall comply with the following standards when authorizing the disclosure or commercial export of any information, classified or unclassified, relating to sales, leases, loans, or grants of military equipment:

6.4.1. Release Authorization. Before approval of initiatives that could lead to a sale, lease, loan, or grant of military equipment, obtain authorization from the appropriate designated disclosure authority for disclosure of all necessary classified equipment and information required for system operation, employment, maintenance, and training, including system software.

6.4.2. Initial Disclosures. Limit initial disclosures to general information, usually no higher than CONFIDENTIAL, on system characteristics, capabilities, and price and availability until a sale, lease, loan, or grant is consummated.

6.4.3. System Countermeasures. Withhold specific information on system countermeasures susceptibilities or vulnerabilities and counter-countermeasures capabilities, until the sale, lease, loan, or grant is consummated.

6.4.4. Operation, Employment, Maintenance, and Training. After consummation of a sale, lease, loan, or grant, classified military information may be disclosed up to the level necessary for operation, employment, maintenance, and training.

6.4.5. Data Packages. Edit or rewrite data packages to exclude information that is beyond that which has been authorized for disclosure.

6.4.5.1. The disclosure of technical data for production purposes shall be limited to data that is necessary to produce a specific item that is approved for release to the country that is to receive the data.

6.4.5.2. The disclosure of technical data for maintenance purposes shall be limited to data that is necessary to perform the level of maintenance that has been authorized for the country that is to receive the data.

6.5. Foreign Test and Evaluation

6.5.1. Foreign test and evaluation of the U.S. classified equipment may be authorized when the tests:

6.5.1.1. Are on an item approved for foreign disclosure by the appropriate disclosure authority.

6.5.1.2. Can be performed at a U.S. installation or under other strict U.S. control that guarantees appropriate safeguards for classified information and classified or unclassified critical technology.

6.5.2. Exceptions to subparagraph 6.5.1.2., above, such as the transfer of a single classified military item for test and evaluation under foreign security control, may be authorized only when all of the following conditions are fulfilled:

6.5.2.1. There is no transfer of, and the test will not reveal, technology that the United States would not license for manufacture in the foreign country.

6.5.2.2. There is no release of equipment that would not be approved for foreign sale or export to the foreign country, if requested.

6.5.2.3. The release will result in a clearly defined advantage to the United States; for example:

6.5.2.3.1. Specifically defined avoidance of significant costs or acceleration of programs in development efforts by the United States and its allies.

6.5.2.3.2. Advance the objectives of standardization with and among U.S. allies by promoting cooperation in research and development.

6.5.2.3.3. Exchange technical and scientific information of common interest on a mutually beneficial basis.

6.5.2.4. The Secretary of the Military Department concerned, in coordination with the Office of the Under Secretary of Defense (Acquisition), approves the exception as meeting the described conditions in paragraph 6.5.2., above. The Chair of the NDPC shall be informed of each exception; the Chair shall notify the NDPC members.

6.5.2.5. The test is performed under a test and evaluation agreement negotiated under DoD Directive 5530.3 (reference (h)), or a lease arrangement or sales contract containing requisite security controls.

6.5.2.6. The releases are reported to the FORDTIS.

6.6. Foreign Participation in DoD Component Classified Training Activities

6.6.1. Receiving Training on U.S. Equipment. A foreign national may receive training on U.S. equipment that is classified or involves classified information, if the equipment is in the inventory of or is to be acquired by the trainee's government after the following:

6.6.1.1. The prospective trainee's government has concluded an international agreement or signed a purchase agreement with the United States to acquire the equipment and training; or

6.6.1.2. The Defense Security Assistance Agency has issued an International Military Education and Training (IMET) order for the training.

6.6.2. Conducting Training on U.S. Equipment. A foreign national may conduct training on U.S. equipment that is classified or involves classified information, if the item has been sold or otherwise provided to the foreign national's government and the U.S. Government has specifically approved the provisions of such training to any third party that is involved.

6.6.3. Third-Country Equipment. Foreign nationals may receive or conduct training on equipment provided by a third-country that is classified or involves third-country classified information only with the prior written consent of the government that provided the equipment.

6.7. Requests for Classified Documents

6.7.1. Disclosure Review. Requests for classified documents by a foreign representative shall be forwarded to the applicable designated disclosure authority of the originating DoD Component for review and approval or denial. The requests shall be processed using the FORDTIS, when practicable.

6.7.2. Report to the FORDTIS. The designated disclosure authority that renders the decision shall report it to the FORDTIS under DoD Instruction 5230.18 (reference (i)).

6.7.3. Reference Lists and Bibliographic Material. To avoid false impressions and to avoid proliferation of requests for classified military information that is not releasable to the requestor, the DoD Components shall:

6.7.3.1. When practical, excise references to nonreleasable documents and information from material that may be otherwise released.

6.7.3.2. Discourage release of documents that are reference lists or are bibliographic. To react favorably to justified foreign requests for information, identify the requestor's specific requirements and provide only the U.S. information that satisfies that requirement and is determined to be releasable.

6.8. Foreign Access to Information When Participating in U.S. Procurement Programs. Participation consistent with applicable U.S. laws, regulations, and security requirements in DoD procurement initiatives by contractors from countries with which the Department of Defense has agreements that encourage reciprocal participation in defense procurement may include access to classified information consistent with this Directive as follows:

6.8.1. Access to Technical Data. Qualified government and industry representatives from those countries shall be given appropriate access to technical data, consistent with this Directive and the ITAR (reference (f)), necessary to bid on the DoD contracts.

6.8.2. Disclosure Decisions. Disclosure decisions involving those countries shall be made before the announcement of the procurement (see subsection 4.6., above), and the announcement shall describe any restrictions on foreign participation.

6.8.3. Participation as Subcontractor. When it is determined that foreign contractors are not authorized to participate in the classified or other sensitive aspects of a potential contract, consideration should be given to their requests for participation in unclassified or less sensitive aspects of the contract as a subcontractor.

6.8.4. Requests for Documentation. Requests by foreign entities for classified or controlled unclassified documentation must be submitted through government channels.

6.9. NDPC Operations. The following procedures apply to the activities below:

6.9.1. Exceptions to NDP-1

6.9.1.1. Exceptions to NDP-1 (reference (c)), other than those granted by the Secretary of Defense or the Deputy Secretary of Defense, shall be granted only by the NDPC.

6.9.1.2. All proposed disclosure actions that require decisions by the Secretary of Defense or the Deputy Secretary of Defense shall contain the views of the originating DoD Component or Agency and shall be coordinated with the Chair of the NDPC.

6.9.1.3. When the Secretary of Defense or the Deputy Secretary of Defense grants an exception to policy, the DoD Component originating or participating in the determination shall notify the Chair of the NDPC so that the exception may be recorded properly and reported promptly to the NDPC members and the National Security Council and recorded in the FORDTIS.

6.9.1.4. All other requests for exception to policy shall:

6.9.1.4.1. Be forwarded through channels to the designated disclosure authority who represents the requestor's organization on the NDPC.

6.9.1.4.2. At a minimum, include the information in enclosure 5.

6.9.2. Reporting to the NDPC of Compromises of U.S. Classified Military Information Furnished to Foreign Governments. The DoD Components having knowledge of compromises of U.S. classified information by foreign governments promptly shall inform the originating DoD Component. The originating DoD Component shall conduct a damage assessment and shall provide copies of the completed case report and damage assessment to the Chair of the NDPC. If the originating DoD Component is not known, the Chair of the NDPC shall conduct the damage assessment and prepare the case report. In either situation, the Chair of the NDPC shall provide the NDPC with an evaluation to serve as a basis for determining whether the nature of the compromise requires a change in reference (c).

6.9.3. Operation of the NDPC

6.9.3.1. NDP-1, NDPC Record of Action 001.7/70 (references (c) and (o)), and this Directive govern the DoD Component participation in the NDPC operations.

6.9.3.2. The DoD Components shall provide qualified personnel to participate on the NDPC security survey teams, when requested. The parent DoD Component shall bear travel and per diem expenses for participants.

6.9.3.3. The DoD members of NDPC security survey teams shall

participate in pre-departure briefings, all scheduled team activities, and the preparation of all reports and briefings resulting from the security survey.

6.9.4. Cooperation with the NDPC. Under the NDP-1 (reference (c)), the Chair of the NDPC acts for and in the name of the Secretary of Defense in carrying out the decisions of the NDPC. All of the DoD Components shall support the Chair's requests for assistance in disclosure matters.

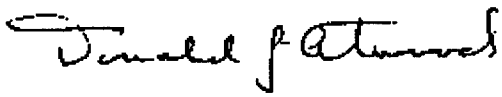
6.10. Classification Requirements. DoD 5200.1-R (reference (j)) governs classification and safeguarding of classified information. The DoD Components also shall follow the security classification guide for NDP matters in enclosure 6.

7. INFORMATION REQUIREMENTS

The reports referenced in this Directive are exempt from licensing in accordance with paragraph 5.4.2. of DoD 7750.5-M (reference (p)).

8. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Policy within 120 days.



Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 6

1. References, continued
2. Definitions
3. NDP-1 Disclosure Criteria, Conditions, and Limitations
4. The DDL
5. Requests for Exception to Policy
6. Security Classification Guide for NDP

E1. ENCLOSURE 1

REFERENCES, continued

(d) DoD Directive C-5230.23, "Intelligence Disclosure Policy (U)," November 18, 1983

(e) DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984

(f) Title 22, Code of Federal Regulations, Parts 120-130, "International Traffic in Arms Regulations (ITAR)"

(g) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991

(h) DoD Directive 5530.3, "International Agreements," June 11, 1987

(i) DoD Instruction 5230.18, "The DoD Foreign Disclosure and Technical Information System (FORDTIS)," November 6, 1984

(j) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(k) Public Law 83-703, "Atomic Energy Act of 1954," August 30, 1954, as amended (Sections 2121, 2153, and 2164 of title 42, United States Code)

(l) DoD 7110.1-M, "Department of Defense Budget Guidance Manual," May 1990, authorized by DoD Instruction 7110.1, October 30, 1980

(m) DoD Directive 5200.12, "Conduct of Classified Meetings," May 16, 1988

(n) DoD Directive 5230.20, "Control of Foreign Representatives," June 25, 1984

(o) National Military Information Disclosure Policy Committee Record of Action 001.7/70, "NDPC Detailed Operating Procedures," September 15, 1981

(p) DoD 7750.5-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by DoD Directive 7750.5, August 7, 1986

(q) Executive Order 12356, "National Security Information," April 2, 1982

(r) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

(s) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988

(t) Title 15, Code of Federal Regulations, Parts 730-799, "Export Administration Regulations (EAR)"

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Classified Military Equipment. Military equipment that is itself classified; contains classified information that may be derived from or revealed by its operation or testing; or will require the disclosure of classified information for operation, employment, maintenance, or training.

E2.1.2. Classified Military Information. Information originated by or for the Department of Defense or its Agencies or is under their jurisdiction or control and that requires protection in the interests of national security. It is designated TOP SECRET, SECRET, and CONFIDENTIAL, as described in E.O. 12356 (reference (q)). Classified military information may be in oral, visual, or material form and has been subdivided further into the eight categories described below:

E2.1.2.1. Category 1 - Organization, Training, and Employment of Military Forces. Information of a general nature pertaining to tactics, techniques, tactical doctrine, and intelligence and counterintelligence doctrine and techniques. Excluded is information necessary for the operation, training, and maintenance on specific equipment covered under Categories 2 and 3, below.

E2.1.2.2. Category 2 - Military Materiel and Munitions. Information on specific items of equipment already in production, or in service, and the information necessary for the operation, maintenance, and training. Items on the U.S. Munitions List fall within this category. This category does not pertain to equipment that is in research and development.

E2.1.2.3. Category 3 - Applied Research and Development Information and Materiel. Information related to fundamental theories, design, and experimental investigation into possible military applications; it includes engineering data, operational requirements, concepts, and military characteristics required to adopt the item for production. Development ceases when the equipment has completed suitability testing and has been adopted for use or production.

E2.1.2.4. Category 4 - Production Information. Information related to designs, specifications, manufacturing techniques, and such related information necessary to manufacture materiel and munitions.

E2.1.2.5. Category 5 - Combined Military Operations, Planning, and Readiness. Information necessary to plan, ensure readiness for, and provide support to the achievement of mutual force development goals or participation in specific combined tactical operations and exercises. It does not include strategic plans and guidance or North American defense information.

E2.1.2.6. Category 6 - U.S. Order of Battle. Information pertaining to U.S. forces in a specific area. In general, disclosures of this information are limited to those countries in which U.S. forces are stationed or are in adjacent geographical areas.

E2.1.2.7. Category 7 - North American Defense. Information related to plans, operations, programs, and projects, to include data and equipment, directly related to North American defense.

E2.1.2.8. Category 8 - Military Intelligence. Information of a military character pertaining to foreign nations. This category of information does not include national intelligence or sensitive compartmented information under the purview of the Director of Central Intelligence (DCI).

E2.1.3. Controlled Unclassified Information. Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulations of the originating country. It includes U.S. information that is determined to be exempt from public disclosure in accordance with DoD Directives 5230.25 and 5400.7 (references (r) and (s)) or that is subject to export controls in accordance with the ITAR (reference (f)) or the EAR (reference (t)).

E2.1.4. Delegation of Disclosure Authority Letter (DDL). A letter issued by the appropriate designated disclosure authority explaining classification levels, categories, scope, and limitations of information under a DoD Component's disclosure jurisdiction that may be disclosed to a foreign recipient. It is used to delegate disclosure authority to subordinate disclosure authorities.

E2.1.5. Designated Disclosure Authority. An official, at subordinate component level, designated by the Head of a DoD Component or the Component's Principal Disclosure Authority to control disclosures of classified military information by his or her organization.

E2.1.6. Disclosure. Conveying classified information, in any manner, to an authorized representative of a foreign government.

E2.1.7. Foreign Disclosure and Technical Information System (FORDTIS). An automated system to assist decision makers and analysts in reviewing, coordinating, and reaching decisions concerning proposals to release classified military information, materiel, and technology to foreign governments.

E2.1.8. Government-to-Government Channels. The principle that classified information and materiel will be transferred by government officials through official channels or through other channels expressly agreed upon by the governments involved. In either case, the information or materiel may be transferred only to a person specifically designated in writing by the foreign government as its representative for that purpose.

E2.1.9. Intelligence. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

E2.1.10. International Organization. An entity established by recognized governments pursuant to an international agreement which, by charter or otherwise, is able to acquire and transfer property, make contracts and agreements, obligate its members, and pursue legal remedies.

E2.1.11. Joint Information. Military information over which two or more DoD Components, or two or more Federal Departments or Agencies, exercise control, jurisdiction, or security awareness.

E2.1.12. Meeting. A conference, seminar, symposium, exhibit, convention, training course, or other gathering during which classified or controlled unclassified information is disclosed.

E2.1.13. Originating DoD Component. The DoD Agency that exercises original classification jurisdiction for classified information.

E2.1.14. Security Assurance. The written confirmation, requested by and exchanged between governments, of the security clearance level or eligibility for clearance, of their employees, contractors, and citizens. It includes a statement by a responsible official of a foreign government that the original recipient of U.S. classified military information possesses the requisite security clearance and is approved by his or her government for access to information of the security classification involved on behalf of the foreign government and that the recipient will comply with any security requirements specified by the United States. In the case of

industrial facilities, the security assurance should include a statement concerning the level of storage capability.

E2.1.15. Sensitive Compartmented Information. Information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.

E2.1.16. Strategic War Plan. A plan for the overall conduct of a war.

E3. ENCLOSURE 3

NDP-1 DISCLOSURE CRITERIA, CONDITIONS, AND LIMITATIONS

E3.1.1. Disclosure Criteria. Disclosures of classified military information in Categories 1 through 8 defined in item E2.1.2. of enclosure 2 may be made only when all of the criteria listed in subsections E3.1.1.1. through E3.1.1.5., below, are satisfied. Disclosures in Category 8 also must be in compliance with DoD Directive C-5230.23 (reference (d)).

E3.1.1.1. Disclosure is consistent with U.S. foreign policy and national security objectives concerning the proposed recipient foreign government. For example:

E3.1.1.1.1. The recipient government cooperates with the United States in pursuance of military and political objectives that are compatible with those of the United States.

E3.1.1.1.2. A specific U.S. national purpose, diplomatic or military, will be served.

E3.1.1.1.3. The information will be used in support of mutual defense and security objectives.

E3.1.1.2. Disclosure is consistent with U.S. military and security objectives. For example:

E3.1.1.2.1. Disclosures of advanced technology, if compromised, will not constitute an unreasonable risk to the U.S. position in military technology and operational capabilities, regardless of the intended recipient.

E3.1.1.2.2. The proposed disclosure reflects the need for striking a proper balance between pursuit of our mutual defense and foreign policy objectives on the one hand and the preservation of the security of our military secrets on the other.

E3.1.1.3. The foreign recipient of the information will afford it substantially the same degree of security protection given to it by the United States. (The intent of a foreign government to protect U.S. classified military information is established in part by the negotiation of a General Security of Information Agreement or other similar security arrangement. A foreign government's capability to protect U.S. classified

military information normally is determined by the evaluation of embassy security assessments, Central Intelligence Agency risk assessments, National Military Information Disclosure Policy Committee (NDPC) Security Survey Reports, and/or historical precedence.)

E3.1.1.4. Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed. For example:

E3.1.1.4.1. The United States obtains information from the recipient nation on a quid pro quo basis.

E3.1.1.4.2. The exchange of military information or participation in a cooperative project will be advantageous to the United States from a technical or other military viewpoint.

E3.1.1.4.3. The development or maintenance of a high level of military strength and effectiveness on the part of the government receiving the information will be advantageous to the United States.

E3.1.1.5. The disclosure is limited to information necessary to the purpose for which disclosure is made. For example, if the purpose of the disclosure is the sale of military equipment, information on operation, maintenance, and training would be released. Research and development data, or production know-how, must be withheld.

E3.1.2. Disclosure Conditions. After a decision is made to disclose classified military information to a foreign government or international organization, based on the criteria listed in subsections E3.1.1.1. through E3.1.1.5. of this enclosure, above, or an exception to policy, release of the classified military information will be contingent upon agreement by the recipient foreign government that the listed minimal conditions in subsections E3.1.2.1. through E3.1.2.8., below, will be met. The conditions normally are satisfied by the provisions of existing General Security of Information Agreements. When a General Security of Information Agreement does not exist, the conditions may be included in a program-specific agreement, government contract, or similar arrangement.

E3.1.2.1. The information or acknowledgment of its possession will not be revealed to a third-country government, organization, or person, except with the prior written permission of the originating U.S. Department Agency.

E3.1.2.2. The information will be afforded substantially the same degree of security protection afforded to it by the United States.

E3.1.2.3. The information will be used only for designated military purposes, or other specified purposes.

E3.1.2.4. The recipient will report promptly and fully to U.S. authorities any known or suspected compromise of U.S. classified military information released to it.

E3.1.2.5. All individuals and facilities that will have access to the classified military information and materiel will have security clearances granted by their government at a level equal to that of the classified information involved and an official need-to-know.

E3.1.2.6. The information will be transferred through government-to-government channels.

E3.1.2.7. Security experts of each government will be permitted to visit the other government, when mutually convenient, to review and discuss each other's policies and practices for protecting classified information.

E3.1.2.8. The recipient of the information agrees to abide by or meet U.S.-specified special terms and conditions for the release of U.S. information or materiel.

E3.1.3. Disclosure Limitations

E3.1.3.1. General Limitations. Nothing in this Directive shall be construed so as to allow the disclosure of the following types of information:

E3.1.3.1.1. Prohibited by Law or Agreement. Classified information, the disclosure of which is prohibited by Federal law or by any international agreement to which the United States is a party.

E3.1.3.1.2. Naval Nuclear Information. Any naval nuclear propulsion information, classified or unclassified, except under an agreement negotiated pursuant to the Atomic Energy Act of 1954, as amended (reference (k)).

E3.1.3.1.3. Proprietary Information. Classified or unclassified proprietary information, the rights to which are owned by private firms or citizens (i.e., patents, copyrights, or trade secrets) without the owner's consent, unless such disclosure is authorized by relevant legislation, and then release will be subject to such legislation.

E3.1.3.1.4. National Intelligence. National Intelligence or interdepartmental intelligence produced within the National Foreign Intelligence Board (NFIB) structure. Such intelligence cannot be disclosed without authorization of the DCI in accordance with applicable policies.

E3.1.3.1.5. National Security Telecommunications and Information Systems Security Information. The National Security Telecommunications and Information Systems Security Committee is authorized by its terms of reference to make disclosures of classified military telecommunications and information systems security equipment and information without reference to the NDPC.

E3.1.3.1.6. Counterintelligence. Operational information related to counterintelligence activities and disclosures related thereto.

E3.1.3.1.7. Atomic Information. Such disclosures are made in accordance with the Atomic Energy Act of 1954, as amended (reference (k)).

E3.1.3.1.8. Strategic Planning and Guidance. Only the Secretary of Defense or the Deputy Secretary of Defense may authorize the disclosure of plans, concepts, or other information about strategic war plans. Requests for such disclosure shall be submitted through the Chairman of the Joint Chiefs of Staff.

E3.1.3.2. Specifically Prohibited Disclosures. The following types of classified information are specifically prohibited from disclosure:

E3.1.3.2.1. Classified information officially obtained from a foreign government, except when the information has been conveyed by the government with express written consent to its further disclosure.

E3.1.3.2.2. Combined information without prior agreement of all parties.

E3.1.3.2.3. Joint information without prior agreement of all Departments or Agencies having control or jurisdiction.

E3.1.3.2.4. Information originated by or for another Department or Agency, unless that Department or Agency consents to the disclosure.

E3.1.3.2.5. Intelligence information described in section I, subparagraph 5.c.(2) and section II, subparagraph 5.b.(7) of NDP-1 (reference (c)).

E4. ENCLOSURE 4

THE DDL

The following DDL format should be used by the DoD Components: (While all elements identified should be provided in the general order shown, information should be presented in the clearest and easiest-to-use manner. For example, the usefulness of the DDL for complex systems will be enhanced if items 5 and 6 are broken out by major subsystems and software and disclosures are discussed separately.)

TITLE: DATE:

1. CLASSIFICATION: Identify highest classification of information to be disclosed.

2. DISCLOSURE METHODS: E.g., oral, visual, or documentary.

3. CATEGORIES PERMITTED: Specify National Disclosure Policy categories to be disclosed.

4. SCOPE: Specify who is authorized to release material or information, and to whom disclosure is authorized.

5. AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that can be released or disclosed.

6. NOT AUTHORIZED FOR RELEASE AND/OR DISCLOSURE: Describe materiel and/or information that cannot be released or disclosed. (In addition to providing specific descriptions of releasable and restricted materiel and information, items 5 and 6 will also specify any conditions or limitations to be imposed; e.g., time-phasing of release, allowable forms for software, identification of items releasable only as finished, tested assemblies, etc.)

7. PROCEDURES: Specify review and release procedures, special security procedures, or protective measures to be imposed.

8. REDELEGATION: Specify the extent of redelegation of authority (if any) permitted to subordinate activities.

E5. ENCLOSURE 5

REQUESTS FOR EXCEPTION TO POLICY

Requests for an exception to policy shall contain the following elements of information:

E5.1.1. A concise statement of the action proposed. Include security classification and categories of U.S. classified military information to be disclosed. (For example: "The OUSD(A) member, National Disclosure Policy Committee (NDPC), requests an exception to the National Disclosure Policy to permit the disclosure of SECRET Category 3 (Applied Research and Development Information and Materiel) information to the Government of _____ in support of the negotiation of a Data Exchange Agreement pertaining to surface-to-air missiles.")

E5.1.2. A precise statement of why an exception to policy is required. (For example: An exception is required because (a) the level of classified information involved exceeds the classification level delegated in Annex A of NDP-1; or (b) the proposed action is not in consonance with policy currently established in Annex B or C of NDP-1; or (c) certain (identify which) of the disclosure criteria or conditions listed in section II. of NDP-1 are not fully met; or (d) any or all of the above in combination.)

E5.1.3. An assessment of how each of the disclosure criteria and conditions in section II. of NDP-1 shall be met:

E5.1.3.1. "Disclosure is consistent with the foreign policy of the United States toward the Government of _____." (A further detailed discussion shall be included to substantiate this statement. Reference shall be made to Presidential, National Security Council, or other high-level policy decisions to support the justification provided. A simple statement such as "the recipient cooperates with the United States in pursuance of military and political objectives" is not sufficient.)

E5.1.3.2. "The military security of the United States permits disclosure." (If equipment or technology is involved, there must be a discussion on the result of a compromise on U.S. operational capability or the U.S. position in military technology. This discussion shall include an analysis of the state of the art regarding the technology involved, the susceptibility of the item to reverse engineering, the capability of the foreign recipient to reverse engineer the item, the foreign availability

of the technology or equipment involved, and other governments to whom similar equipment or technology has been released.)

E5.1.3.3. "The foreign recipient will afford the information substantially the same degree of security protection given to it by the United States." (If there has been an NDPC Security Survey for the proposed recipient, the conclusion reached therein shall be discussed. In the absence of an NDPC Security Survey, efforts shall be made to obtain, through intelligence channels, a counterintelligence risk assessment or security analysis of the foreign government's security capabilities. The mere statement that "classified information has been released previously to this government and there is no indication that such information has been compromised" is not sufficient.)

E5.1.3.4. "Disclosures will result in benefits to the United States at least equivalent to the value of the information disclosed." (For example: (1) if the United States obtains information from the proposed recipient on a quid-pro-quo basis, describe the information and the value to the United States; (2) explain how the exchange of military information for participation in a cooperative project will be advantageous to the United States from a technical or military capability viewpoint; (3) if the development or maintenance of a high degree of military strength and effectiveness on the part of the recipient government will be advantageous to the United States, explain how.)

E5.1.3.5. "The disclosure is limited to information necessary to the purpose for which disclosure is made." (For example, if the purpose of the request is for the sale of equipment only, it shall be indicated clearly that research and development data or production know-how is not to be divulged or that documentation will be sanitized.)

E5.1.4. Any limitations placed on the proposed disclosure in terms of information to be disclosed, disclosure schedules, or other pertinent caveats that may affect NDPC approval or denial of the request. (If disclosures are to be phased or if certain information is not to be released, the phasing or nonreleasable information shall be specified.)

E5.1.5. A statement that the requested exception is to be either a continuing exception, subject to annual review, or a one-time exception. (A continuing exception usually is associated with a long-term project, such as a coproduction program or military sale when the United States will be obligated to provide life-cycle support. A one-time exception typically is used for a briefing or demonstration or short-term training.)

E5.1.6. The names and titles of U.S. officials accredited to the requesting foreign government or international organization with whom the proposed exception has been coordinated, as well as the views of the Theater Commander. (Sufficient time shall be allowed to obtain an opinion from U.S. Embassy personnel in-country and the responsible Theater Commander before submitting the request for approval. Many cases are delayed because a U.S. Embassy or Theater Commander opinion has not been obtained.)

E5.1.7. The opinion of other interested Departments or Agencies if joint Service or shared information is involved. (If the information or item of equipment is of shared or joint interest, such as an air-to-air missile used by two Services or containing technology of concern to another Service, the views of the other party will be included.)

E5.1.8. Any information not mentioned above that would assist the NDPC members, the Secretary of Defense, or the Deputy Secretary of Defense in evaluating the proposal.

E5.1.9. The name and telephone number of a knowledgeable individual within the requesting organization who can provide additional technical detail or clarification concerning the case at issue.

E5.1.10. The date a response is desired on the case. Ten full working days for NDPC case deliberations should be allowed. The suspense date (10 full working days) is computed starting from the first full working day after the date of the request.

E6. ENCLOSURE 6

SECURITY CLASSIFICATION GUIDE FOR NATIONAL DISCLOSURE POLICY

SUBJECT MATTER	CLASSIFICATION	REMARKS
A. The Charts in Annex A of NDP-1 (reference (c)).	SECRET	
1. The association of a foreign country or international organization with one or more disclosure category entries quoted from the chart in Annex A of reference (c).	CONFIDENTIAL	
2. The association of one or more disclosure category entries in the charts in Annex A of reference (c) pertaining to two or more foreign countries or international organizations (that is, any comparison of the disclosure levels of two or more countries or international organizations).	SECRET	
B. The fact that a specific foreign country or international organization has agreed to afford U.S. classified military information the same degree of protection as afforded by the U.S. Government.	UNCLASSIFIED	Unless the mere existence of the governing security agreement is classified, in which case the same classification applies. This can be determined by reviewing Part B of the charts in Annex A of reference (c).
C. Disclosure authority as set forth in section II.4. of reference (c).	UNCLASSIFIED	
D. Disclosure criteria (and examples) set forth in section II.5.a. of reference (c) without reference to a specific case or country.	UNCLASSIFIED	
E. Disclosure criteria for military intelligence as set forth in section II.5.b. of NDP-1 (reference (c)) and DoD Directive C-5230.23 (reference (d)).	CONFIDENTIAL	Unless otherwise specified by the paragraph markings in section II.5.b.
F. Disclosure conditions for classified military information as set forth in section II.6. of reference (c).	UNCLASSIFIED	
G. NDPC organization and membership in section III. of reference (c).	UNCLASSIFIED	
H. NDPC procedures enumerated in section IV. of reference (c).	UNCLASSIFIED	Except for section IV.2.b. which is CONFIDENTIAL
I. Specific disclosure policy, in addition to that in the chart in Annex A of reference (c), relative to a specific country or international organization.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
J. Specific disclosure policy for selected weapon systems, equipment, and technologies.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
K. Information revealing the security policies, procedures, methods, or practices of a foreign country or international organization for protecting classified military information compiled by a NDPC Security Survey Team.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.

SUBJECT MATTER	CLASSIFICATION	REMARKS
L. Assessments, including deficiencies or recommendations, compiled by an NDPC Security Survey Team that would not result in adverse effects of foreign relations if disclosed but that could result in damage to the national defense if disclosed but that could result in damage to the national defense if disclosed. For example, the deficiency concerns an exploitable vulnerability that, if revealed, could cause direct or immediate jeopardy to the security of U.S. classified information.	CONFIDENTIAL	Other classification levels will be recommended to the Chair of the NDPC when circumstances warrant.
M. Deficiencies or recommendations compiled by the NDPC Security Team that could result in adverse effects on foreign relations if disclosed.	CONFIDENTIAL	Other classification levels will be recommended to the Chairman of the NDPC when circumstances warrant.

N. The above items shall be declassified on "ODAR."

This Page Intentionally Left Blank

DoDD 5230.24

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 5230.24

March 18, 1987

USD(A)

SUBJECT: Distribution Statements on Technical Documents

References: (a) DoD Directive 5230.24, subject as above, November 20, 1984 (hereby canceled)
(b) DoD Directive 3200.12, "DoD Scientific and Technical Information Program," February 15, 1983
(c) through (i), see enclosure E1.

1. REISSUANCE AND PURPOSE

This Directive reissues reference (a) to update policies and procedures for marking technical documents, including production, engineering, and logistics information, to denote the extent to which they are available for distribution, release, and dissemination without additional approvals or authorizations.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments (including their National Guard and Reserve components), the Organization of the Joint Chiefs of Staff (OJCS), the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2.2. Covers newly created technical documents generated by all DoD-funded research, development, test and evaluation (RDT&E) programs, which are the basis of the DoD Scientific and Technical Information Program (STIP) described in reference (b). This Directive also 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 such equipment.

2.3. Facilitates implementation of DoD Directive 5230.25 (reference (c)) by enabling document originators to signify to what extent technical documents must be controlled in accordance with procedures of that Directive.

2.4. Does not apply to technical documents categorized as cryptographic and communications security, communications and electronic intelligence, and such other categories that may be designated by the Director, National Security Agency/Chief, Central Security Service.

2.5. May not be used by DoD Components as authority to deny information to Congress, or to any Federal, State, or local governmental agency that requires such data for regulatory or other official governmental purposes. When the information is otherwise subject to DoD distribution controls, the recipient shall be so notified.

2.6. Does not provide authority to withhold from public disclosure unclassified information regarding DoD operations, policies, activities, or programs, including the costs and evaluations of performance and reliability of military and space equipment, or any other information not exempt from release under DoD 5400.7-R (reference (d)).

2.7. Does not establish non-recurring charges that may apply to recipients of DoD technical data. Such charges are determined in accordance with DoD Directive 2140.2 (reference (e)).

3. DEFINITIONS

The terms used in this Directive are defined in enclosure E2.

4. POLICY

It is DoD policy to pursue a coordinated and comprehensive program to provide for a strong and viable military research, acquisition, and support program consistent with requirements of national security, export laws, and competitive procurement.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Acquisition (USD(A)) shall monitor compliance with this Directive within DoD Components and take such actions that may be required to ensure consistent and appropriate implementation and control of information within the scope of this Directive.

5.2. The Under Secretary of Defense for Policy (USD(P)) shall prepare and issue, as required, policy guidance regarding the dissemination and control of information within the scope of this Directive.

5.3. The Assistant Secretary of Defense (Public Affairs) (ASD(PA)) shall ensure that technical material submitted for public release clearance under DoD Directive 5230.9 (reference (f)) is properly reviewed to determine whether the information is appropriate for Distribution Statement A (enclosure E3.) and shall inform the submitter of distribution limitations recommended if public release is not approved. The ASD(PA) shall also process appeals when public release denial is based upon this Directive.

5.4. The General Counsel, Department of Defense (GC, DoD), shall assist in carrying out this Directive by advising DoD Components regarding the statutory and regulatory requirements governing the export or other dissemination of technical data.

5.5. Heads of DoD Components shall ensure that this Directive is implemented within their respective Components in a uniform, consistent manner and shall establish procedures to ensure that technical documents are marked correctly.

6. PROCEDURES

6.1. All DoD Components generating or responsible for technical documents shall determine their distribution availability and mark them appropriately before primary distribution. Documents recommended for public release must first be reviewed in accordance with DoD Directive 5230.9 (reference (f)).

6.2. DoD distribution statement markings shall not be required on technical proposals or similar documents submitted by contractors seeking DoD funds or contracts.

6.3. Managers of technical programs shall assign appropriate distribution statements to technical documents generated within their programs to control the secondary distribution of those documents.

6.3.1. All newly created unclassified DoD technical documents shall be assigned distribution statement A, B, C, D, E, F, or X (see enclosure E3.).

6.3.2. Classified DoD technical documents shall be assigned distribution statement B, C, D, E, or F. The distribution statement assigned to a classified document shall be retained on the document after its declassification or until changed specifically or removed by the controlling DoD office. Technical documents that are declassified and have no distribution statement assigned shall be handled as distribution statement F documents until changed by the controlling DoD office.

6.3.3. Scientific and technical documents that include a contractor-imposed limited rights statement shall be marked and controlled in accordance with subpart 27.4 of the DoD Supplement to the FAR (reference (g)).

6.3.4. For each newly generated technical document, managers of technical programs shall determine whether the document contains export-controlled technical data; DoD Directive 5230.25 (reference (c)) provides guidance for making this determination. Additional guidance may be obtained from Component legal counsel. All documents that are found to contain export-controlled technical data shall be marked with the export control statement contained in subsection E3.1.1.8., below, of enclosure E3.; any document so marked must also be assigned distribution statement B, C, D, E, F, or X.

6.3.5. Technical documents in preliminary or working draft form shall not be disseminated without a proper security classification review and assignment of a distribution statement as required by this Directive.

6.4. Distribution statements shall remain in effect until changed or removed by the controlling DoD office. Each controlling DoD office shall establish and maintain a procedure to review technical documents for which it is responsible to increase their availability when conditions permit. The controlling DoD office shall obtain public release determinations in accordance with reference (f). If public release clearance is obtained, the controlling DoD office shall assign distribution statement A, cancel any other distribution statement, and notify the proper document handling facilities.

6.5. Technical documents marked with superseded distribution statements shall be reviewed when a request for the document is received and shall be assigned an appropriate distribution statement.

6.6. Technical documents in information repositories that have superseded

distribution statements shall be converted as follows:

6.6.1. Documents bearing distribution statement A or B of canceled DoD Directive 5200.20, September 24, 1970, and documents bearing distribution statement A, B, C, D, E, or F contained in Secretary of Defense Memorandum "Control of Unclassified Technology with Military Application," October 18, 1983, need not be reevaluated.

6.6.2. Technical documents bearing distribution statement numbers 2, 3, 4, and 5 of superseded DoD Directive 5200.20, March 29, 1965, shall be assigned, respectively, distribution statements, C, B, E, and F.

6.7. Controlling DoD offices shall notify the Defense Technical Information Center (DTIC) and other proper technical document dissemination facilities promptly when:

6.7.1. Addresses of designated controlling DoD offices are changed.

6.7.2. The controlling DoD office is redesignated.

6.7.3. Classification markings, distribution statements, or export control statements are changed.

6.8. The distribution statement shall be displayed conspicuously on technical documents so as to be recognized readily by recipients.

6.8.1. For standard written or printed material, the following applies:

6.8.1.1. The distribution statement shall appear on each front cover, title page, and DD Form 1473, "Report Documentation Page."

6.8.1.2. When possible, parts that contain information creating the requirement for a distribution statement shall be prepared as an appendix to permit broader distribution of the basic document.

6.8.1.3. When practical, the abstract of the document, the DD Form 1473 and bibliographic citations shall be written in such a way that the information will not be subject to distribution statement B, C, D, E, F, or X. If the technical information is not prepared in the form of an ordinary document (such as this Directive) and does not have a cover or title page (such as forms and charts), the applicable distribution statement shall be stamped, printed, written, or affixed by other

means in a conspicuous position.

7. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward one copy of implementing documents to the Under Secretary of Defense for Acquisition within 120 days.

William H. Taft, IV
Deputy Secretary of Defense

Enclosures - 4

1. References, continued
2. Definitions
3. Distribution Statements for Use on Technical Documents
4. Contractor-Imposed Distribution Statements

E1. ENCLOSURE 1

REFERENCES, continued

(c) DoD Directive 5230.25, "Withholding of Unclassified Technical Data From Public Disclosure," November 6, 1984

(d) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, March 24, 1980

(e) DoD Directive 2140.2, "Recoupment of Nonrecurring Costs on Sales of U.S. Products and Technology," August 5, 1985

(f) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 2, 1982

(g) DoD Supplement to the Federal Acquisition Regulation (FAR), Part 27, Subpart 27.4

(h) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(i) DoD Instruction 7930.2, "ADP Software Exchange and Release," December 31, 1979

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Contractor. An individual or organization outside the U.S. Government who has accepted any type of agreement or order to provide research, supplies, or services to a U.S. Government Agency, including both prime contractors and subcontractors.

E2.1.1.1. Qualified U.S. Contractor. In accordance with DoD Directive 5230.25 (reference (c)), a private individual or enterprise located in the United States whose eligibility to obtain unclassified export-controlled technical data has been established under procedures developed by (USD(A)).

E2.1.1.2. DoD Potential Contractor. An individual or organization outside the Department of Defense declared eligible for DoD information services by a sponsoring DoD activity on the basis of participation in one of the following programs:

E2.1.1.2.1. The Department of the Army Qualitative Requirements Information Program.

E2.1.1.2.2. The Department of the Navy Industry Cooperative Research and Development Program.

E2.1.1.2.3. The Department of the Air Force Potential Contractor Program.

E2.1.1.2.4. The DoD Scientific and Technical Information Program.

E2.1.1.2.5. Any programs similar to those above in use by other DoD Components.

E2.1.2. Contracted Fundamental Research. Research performed under grants or contracts funded by budget category 6.1 (Research), whether performed by universities or industry, or funded by budget category 6.2 (Exploratory Development) and performed on campus at a university.

E2.1.3. Controlling DoD Office. The DoD activity that sponsored the work that generated the technical data or received the technical data on behalf of the Department of Defense and, therefore, has the responsibility for determining the distribution of a

document containing such technical data. For joint sponsorship, the controlling office is determined by advance agreement and may be either a party, group, or committee representing the interested activities or DoD Components.

E2.1.4. Critical Technology. Technology that consists of:

E2.1.4.1. Arrays of design and manufacturing know-how (including technical data).

E2.1.4.2. Keystone manufacturing, inspection, and test equipment.

E2.1.4.3. Keystone materials.

E2.1.4.4. Goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as militarily-critical technology).

E2.1.5. Distribution Statement. A statement used in marking a technical document to denote the extent of its availability for distribution, release, and disclosure without additional approvals or authorizations. A distribution statement marking is distinct from and in addition to a security classification marking assigned in accordance with DoD 5200.1-R (reference (h)).

E2.1.6. Document. Any recorded information regardless of its medium, physical form, or characteristics.

E2.1.7. Foreign Government Information

E2.1.7.1. Information that is:

E2.1.7.1.1. Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation either expressed or implied, that the information or the source of information, or both, be held in confidence.

E2.1.7.1.2. Produced by the United States following or as a result of a joint arrangement with a foreign government or governments or an international organization of governments or any element thereof, requiring that the information, the arrangement, or both, be held in confidence.

E2.1.7.2. Information described in subparagraphs E2.1.7.1.1. and E2.1.7.1.2., above, and in the possession of the Department of Defense is classified information in accordance with reference (h).

E2.1.8. Primary Distribution. The initial targeted distribution of or access to technical documents authorized by the controlling DoD office.

E2.1.9. Scientific and Technical Information. Communicable knowledge or information resulting from or pertaining to conducting and managing a scientific or engineering research effort.

E2.1.10. Secondary Distribution. Release of technical documents provided after primary distribution by other than the originator or controlling office. It includes loaning, allowing the reading of, or releasing a document outright, in whole or in part.

E2.1.11. Technical Data. Recorded information related to experimental, developmental, or engineering works that can be used to define an engineering or manufacturing process or to design, procure, produce, support, maintain, operate, repair, or overhaul material. The data may be graphic or pictorial delineations in media, such as drawings or photographs, text in specifications or related performance or design type documents, or computer printouts. Examples of technical data include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, catalog-item identifications, and related information and computer software documentation.

E2.1.12. Technical Document. Any recorded information that conveys scientific and technical information or technical data. For purposes of this Directive, this includes such informal documents as working papers, memoranda, and preliminary reports when such documents have utility beyond the immediate mission requirement, or will become part of the historical record of technical achievements.

E2.1.13. Technical Information. Information, including scientific information, that relates to research, development, engineering, test, evaluation, production, operation, use, and maintenance of munitions and other military supplies and equipment

E2.1.14. U.S. DoD Contractor. Those U.S. contractors currently holding grants or contracts with the Department of Defense, or those contractors declared eligible for DoD information services by a sponsoring DoD activity on the basis of participation in a DoD Potential Contractor Program.

E3. ENCLOSURE 3

DISTRIBUTION STATEMENTS FOR USE ON TECHNICAL DOCUMENTS

E3.1.1. The following distribution statements and notices are authorized for use on DoD technical documents:

E3.1.1.1. DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

E3.1.1.1.1. This statement may be used only on unclassified technical documents that have been cleared for public release by competent authority in accordance with DoD Directive 5230.9 (reference (f)). Technical documents resulting from contracted fundamental research efforts will 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.

E3.1.1.1.2. Technical documents with this statement may be made available or sold to the public and foreign nationals, companies, and governments, including adversary governments, and may be exported.

E3.1.1.1.3. This statement may not be used on technical documents that formerly were classified unless such documents are cleared for public release in accordance with reference (f).

E3.1.1.1.4. This statement shall not be used on classified technical documents or documents containing export-controlled technical data as provided in DoD Directive 5230.25 (reference (c)).

E3.1.1.2. DISTRIBUTION STATEMENT B. Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).

E3.1.1.2.1. This statement may be used on unclassified and classified technical documents.

E3.1.1.2.2. Reasons for assigning distribution statement B include:

Foreign Government Information	To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information. Information of this type normally is classified at the CONFIDENTIAL level or higher in accordance with DoD 5200.1-R (reference (h)).
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 not be routinely transmitted outside the U.S. Government.
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 DoD Directive 5230.25 (reference (c)).
Test and Evaluation	To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.
Contractor Performance Evaluation	To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.
Premature Dissemination	To protect patent able information on systems or processes in the developmental or concept stage from premature dissemination.
Administrative or Operational Use	To protect technical or operational data or 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 may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.
Software Documentation	Releasable only in accordance with DoD Instruction 7930.2 (reference (i)).
Specific Authority	To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD Component regulatory documents. When filling in the reason, cite "Specific Authority (identification of valid documented authority)."

E3.1.1.3. DISTRIBUTION STATEMENT C. Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).

E3.1.1.3.1. Distribution statement C may be used on unclassified and classified technical documents.

E3.1.1.3.2. Reasons for assigning distribution statement C include:

Foreign Government Information	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Software Documentation.	Same as distribution statement B.
Administrative or Operational Use	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

E3.1.1.4. DISTRIBUTION STATEMENT D. Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

E3.1.1.4.1. Distribution statement D may be used on unclassified and classified technical documents.

E3.1.1.4.2. Reasons for assigning distribution statement D include:

Foreign Government Information	Same as distribution statement B.
Administrative or Operational Use	Same as distribution statement B.
Software Documentation	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

E3.1.1.5. DISTRIBUTION STATEMENT E. Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).

E3.1.1.5.1. Distribution statement E may be used on unclassified and classified technical documents.

E3.1.1.5.2. Reasons for assigning distribution statement E include:

Direct Military Support	The 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 United States. Designation of such data is made by competent authority in accordance with DoD Directive 5230.25 (reference (c)).
Foreign Government Information	Same as distribution statement B.
Proprietary Information	Same as distribution statement B.
Premature Dissemination	Same as distribution statement D.
Test and Evaluation	Same as distribution statement B.
Software Documentation	Same as distribution statement B.
Contractor Performance Evaluation	Same as distribution statement B.
Critical Technology	Same as distribution statement B.
Administrative-Operational Use	Same as distribution statement B.
Specific Authority	Same as distribution statement B.

E3.1.1.6. DISTRIBUTION STATEMENT F. Further dissemination only as

directed by (inserting controlling DoD office) (date of determination) or higher DoD authority.

E3.1.1.6.1. Distribution statement F is normally used only on classified technical documents, but may be used on unclassified technical documents when specific authority exists (e.g., designation as direct military support as in statement E).

E3.1.1.6.2. Distribution statement F is also used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R (reference (h)).

E3.1.1.7. 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 reference (c) (date of determination). Controlling DoD office is (insert).

E3.1.1.7.1. Distribution statement X shall be used on unclassified documents when distribution statements B, C, D, E, or F do not apply, but the document does contain technical data as explained in reference (c).

E3.1.1.7.2. This statement shall not be used on classified technical documents; however, it may be assigned to technical documents that formerly were classified.

E3.1.1.8. Export Control Warning. All technical documents that are 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 in accordance with provisions of DoD Directive 5230.25." When it is technically infeasible to use the entire statement, an abbreviated marking may be used, and a copy of the full statement added to the "Notice To Accompany Release of Export-Controlled Data" required by DoD Directive 5230.25 (reference (c)).

E3.1.1.9. Handling and Destroying Unclassified/Limited Distribution Documents. Unclassified/Limited Distribution documents shall be handled using the same standard as "For Official Use Only (FOUO)" material, and will be destroyed by any method that will prevent disclosure of contents or reconstruction of the document. When local circumstances or experience indicates 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.

E4. ENCLOSURE 4

CONTRACTOR-IMPOSED DISTRIBUTION STATEMENTS

E4.1.1. Part 27, Subpart 27.4 to the DoD Supplement to the Federal Acquisition Regulation (FAR) (reference (g)) stipulates control procedures for contractor-controlled technical data to which the Government has limited rights. In this case, an approved statement from the DoD Supplement to the FAR shall appear on all copies of each document. Unmarked or improperly marked technical documents supplied by a contractor shall be handled in accordance with the DoD Supplement to the FAR. Limited rights information shall be assigned distribution statements B, E, or F.

E4.1.2. The limited rights statement shall remain in effect until changed or canceled under contract terms or with the permission of the contractor, and until the controlling DoD Component notifies recipients of the document that the statement may be changed or canceled. Upon cancellation of the statement, the distribution, disclosure, or release of the technical document shall then be controlled by its security classification or, if unclassified, by the appropriate statement selected from this Directive.

E4.1.3. Reference (g) defines limited rights as the right to use, duplicate, or disclose technical data in whole or in part, by or for the U.S. Government with the expressed limitation that such technical data, without the written permission of the party furnishing such technical data, may not be:

E4.1.3.1. Released or disclosed in whole or in part outside the Government.

E4.1.3.2. Used in whole or in part by the Government for manufacture, or in the case of computer software documentation, for reproduction of the computer software.

E4.1.3.3. Used by a party other than the Government, except for:

E4.1.3.3.1. Emergency repair or overhaul work only by or for the 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 Government shall be made subject to a prohibition against further use, release, or disclosure.

E4.1.3.3.2. Release to a foreign government, as the interest of the United States may require, only for information or evaluation within such government or for emergency repair or overhaul work by or for such government under the conditions of subparagraph E4.1.3.3.1., above.

This Page Intentionally Left Blank

DoDD 5230.25

This Page Intentionally Left Blank

Department of Defense
DIRECTIVE

NUMBER 5230.25
November 6, 1984

Administrative Reissuance Incorporating Change 1, August 18, 1995

USDR&E

SUBJECT: Withholding of Unclassified Technical Data From Public Disclosure

References: (a) Title 10, United States Code, Section 140c, as added by Public Law 98-94, "Department of Defense Authorization Act, 1984," Section 1217, September 24, 1983
(b) Executive Order 12470, "Continuation of Export Control Regulations," March 30, 1984
(c) Public Law 90-629, "Arms Export Control Act," as amended (22 U.S.C. 2751 et. seq.)
(d) through (n), see enclosure E1.

1. PURPOSE

Under reference (a), this Directive establishes policy, prescribes procedures, and assigns responsibilities for the dissemination and withholding of technical data.

2. APPLICABILITY AND SCOPE

2.1. Reference (a) applies to all unclassified technical data with military or space application in the possession of, or under the control of, a DoD Component that may not be exported lawfully without an approval, authorization, or license under E.O. 12470 (reference (b)) or the Arms Export Control Act (reference (c)). However, the application of this Directive is limited only to such technical data that disclose critical technology with military or space application. The release of other technical data shall be accomplished in accordance with DoD Instruction 5200.21 (reference (d)) and DoD 5400.7-R (reference (e)).

2.2. This Directive:

2.2.1. Applies to the Office of the Secretary of Defense (OSD) and activities supported administratively by OSD, the Military Departments, the Organization of the Joint Chiefs of Staff, the Defense Agencies, and the Unified and Specified Commands (hereafter referred to collectively as "DoD Components").

2.2.2. Does not modify or supplant the regulations promulgated under E.O. 12470 (reference (b)) or the Arms Export Control Act (reference (c)) governing the export of technical data, that is, 15 CFR 379 of the Export Administration Regulations (EAR) (reference (f)) and 22 CFR 125 of the International Traffic in Arms Regulations (ITAR) (reference (g)).

2.2.3. Does not introduce any additional controls on the dissemination of technical data by private enterprises or individuals beyond those specified by export control laws and regulations or in contracts or other mutual agreements, including certifications made pursuant to subsection 3.2., below. Accordingly, the mere fact that the Department of Defense may possess such data does not in itself provide a basis for control of such data pursuant to this Directive.

2.2.4. Does not introduce any controls on the dissemination of scientific, educational, or other data that qualify for General License GTDA under subsection 379.3 of the EAR (reference (f)) (see enclosure E3.) or for general exemptions under subsection 125.11 of the ITAR (reference (g)) (see enclosure E4.).

2.2.5. Does not alter the responsibilities of DoD Components to protect proprietary data of a private party in which the Department of Defense has "limited rights" or "restricted rights" (as defined in subsections 9-201(c) and 9-601(j) of the DoD Federal Acquisition Regulation Supplement, reference or which are authorized to be withheld from public disclosure under 5 U.S.C. 552(b) (4) (reference (i)).

2.2.6. Does not pertain to, or affect, the release of technical data by DoD Components to foreign governments, international organizations, or their respective representatives or contractors, pursuant to official agreements or formal arrangements with the U.S. Government, or pursuant to U.S. Government-licensed transactions involving such entities or individuals. In the absence of such U.S. Government-sanctioned relationships, however, this Directive does apply.

2.2.7. Does not apply to classified technical data. After declassification, however, dissemination of such data that are within the scope of subsection 2.1.,

above, is governed by this Directive.

3. DEFINITIONS

3.1. Except for the definition in subsection 3.2., terms used in this Directive are defined in enclosure E2.

3.2. Qualified U.S. contractor. [1] A private individual or enterprise (hereinafter described as a "U.S. contractor") that, in accordance with procedures established by the Under Secretary of Defense for Research and Engineering, certifies, as a condition of obtaining export-controlled technical data subject to this Directive from the Department of Defense, that:

3.2.1. The individual who will act as recipient of the export-controlled technical data on behalf of the U.S. contractor is a U.S. citizen or a person admitted lawfully into the United States for permanent residence and is located in the United States.

3.2.2. Such data are needed to bid or perform on a contract with the Department of Defense, or other U.S. Government Agency, or for other legitimate business purposes [2] in which the U.S. contractor is engaged, or plans to engage. The purpose for which the data are needed shall be described sufficiently in such certification to permit an evaluation of whether subsequent requests for data, pursuant to subsection 5.4.2., below, are related properly to such business purpose.

3.2.3. The U.S. contractor acknowledges its responsibilities under U.S. export control laws and regulations (including the obligation, under certain circumstances, to obtain an export license prior to the release of technical data within the United States) and agrees that it will not disseminate any export-controlled technical data subject to this Directive in a manner that would violate applicable export control laws and regulations.

---

[1] Canadian contractors may be qualified in accordance with this Directive for technical data that do not require a license for export to Canada under section 125.12 of the ITAR (reference (g)) and section 379.4(d) and 379.5(e) of the EAR (reference (f)) by submitting an equivalent certification to the U.S. Department of Defense.

[2] This does not require a contract with or a grant from the U.S. Government.

3.2.4. The U.S. contractor also agrees that, unless dissemination is permitted by subsection 5.8., below, it will not provide access to export-controlled technical data subject to this Directive to persons other than its employees or persons acting on its behalf, without the permission of the DoD Component that provided the technical data.

3.2.5. To the best of its knowledge and belief, the U.S. contractor knows of no person employed by it, or acting on its behalf, who will have access to such data, who is debarred, suspended, or otherwise ineligible from performing on U.S. Government contracts; or has violated U.S. export control laws or a certification previously made to the Department of Defense under the provisions of this Directive.

3.2.6. The U.S. contractor itself is not debarred, suspended, or otherwise determined ineligible by any Agency of the U.S. Government to perform on U.S. Government contracts, has not been convicted of export control law violations, and has not been disqualified under the provisions of this Directive.

When the certifications required by subsections 3.2.5. and 3.2.6., above, cannot be made truthfully, the U.S. contractor may request the certification be accepted based on its description of extenuating circumstances.

4. POLICY

4.1. In accordance with 10 U.S.C. 140c (reference (a)), the Secretary of Defense may withhold from public disclosure, notwithstanding any other provision of law, any technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be exported lawfully without an approval, authorization, or license under E.O. 12470 (reference (b)) or the Arms Export Control Act (reference (c)). However, technical data may not be withheld under this section if regulations promulgated under either the Order or Act authorize the export of such data pursuant to a general, unrestricted license or exemption in such regulations. (Pertinent portions of such regulations are set forth at enclosures E3. and E4.)

4.2. Because public disclosure of technical data subject to this Directive is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest. Unclassified technical data that are not governed by this Directive, unless otherwise restricted, shall continue to be

made available to the public as well as to State and local governments.

4.3. Notwithstanding the authority provided in subsection 4.1., above, it is DoD policy to provide technical data governed by this Directive to individuals and enterprises that are determined to be currently qualified U.S. contractors, when such data relate to a legitimate business purpose for which the contractor is certified. However, when such data are for a purpose other than to permit the requester to bid or perform on a contract with the Department of Defense, or other U.S Government Agency, and the significance of such data for military purposes is such that release for purposes other than direct support of DoD activities may jeopardize an important U.S. technological or operational advantage, those data shall be withheld in such cases.

4.4. This Directive may not be used by DoD Components as authority to deny access to technical data to the Congress, or to any Federal, State, or local governmental agency that requires such data for regulatory or other official governmental purposes. Any such dissemination will include a statement that the technical data are controlled by the Department of Defense in accordance with this Directive.

4.5. The authority provided herein may not be used to withhold from public disclosure unclassified information regarding DoD operations, policies, activities, or programs, including the costs and evaluations of performance and reliability of military and space equipment. When such information does contain technical data subject to this Directive, the technical data shall be excised from that which is disclosed publicly.

4.6. This Directive may not be used as a basis for the release of "limited rights" or "restricted rights" data as defined in subsections 9-201(c) and 9-601(j) of the DoD Federal Acquisition Regulation Supplement (reference (h)) or that are authorized to be withheld from public disclosure under the Freedom of Information Act (FOIA) (reference (i)).

4.7. This Directive may not be used to provide protection for technical data that should be classified in accordance with E.O. 12356 and DoD 5200.1-R (references (j) and (k)).

4.8. This Directive provides immediate authority to cite 5 U.S.C. 552(b) (3) (reference (i)) as the basis for denials under the FOIA (reference (i)) of technical data currently determined to be subject to the provisions of this Directive.

5. PROCEDURES

All determinations to disseminate or withhold technical data subject to this Directive shall be consistent both with the policies set forth in section 4., above, and with the following procedures:

5.1. Requests for technical data shall be processed in accordance with DoD Directive 5230.24 and DoD Instruction 5200.21 (references (l) and (d)). FOIA (reference (i)) requests for technical data subject to this Directive shall be handled in accordance with the procedures established in DoD 5400.7-R (reference (e)). Such FOIA requests for technical data currently determined to be subject to the withholding authority effected by this Directive shall be denied under reference (i), citing the third exemption to mandatory disclosure, and the requester shall be referred to the provisions of this Directive permitting access by qualified U.S. contractors.

5.2. Upon receipt of a request for technical data in the possession of, or under the control of, the Department of Defense, the controlling DoD office shall determine whether such data are governed by this Directive. The determination shall be based on the following:

5.2.1. The office's finding[3] that such data would require an approval, authorization, or license for export under E.O. 12470 (reference (b)) or the Arms Export Control Act (reference (c)), and that such data may not be exported pursuant to a general, unrestricted license (section 379.3, EAR (reference (f)) (see enclosure E3.) or exemption (section 125.11, ITAR (reference (g)) (see enclosure E4.).

5.2.2. The office's judgment that the technical data under consideration disclose critical technology with military or space application. For purposes of making this determination, the Militarily Critical Technologies List (MCTL) (reference (m)) shall be used as general guidance. The controlling DoD office may request assistance in making such a determination from the Office of the Under Secretary of Defense for Research and Engineering (OUSDR&E) in accordance with procedures established by that office.

5.3. The controlling DoD office shall ensure that technical data determined to be governed by this Directive are marked in accordance with DoD Directive 5230.24 (reference (l)).

---

3 May require consultation with the Department of State or the Department of Commerce, as appropriate.

5.4. The controlling DoD office shall authorize release of technical data governed by this Directive to currently qualified U.S. contractors only, as defined in subsection 3.2., above, unless one of the apply:

5.4.1. The qualification of the U.S. contractor concerned has been temporarily revoked in accordance with subsection 5.5., below; or

5.4.2. The requested data are judged to be unrelated to the purpose for which the qualified U.S. contractor is certified. When release of technical data is denied in accordance with this subsection, the controlling DoD office shall request additional information sufficient to explain the intended use of the requested data and, if appropriate, request a new certification (see subsection 3.2., above) describing the intended use of the requested data; or

5.4.3. The technical data are being requested for a purpose other than to permit the requester to bid or perform on a contract with the Department of Defense or other U.S. Government Agency, in which case the controlling DoD office shall withhold such data if it has been determined by the DoD Component focal point (see paragraph 6.5.3., below) that the significance of such data for military purposes is such that release for purposes other than direct support of DoD-approved activities may jeopardize an important technological or operational military advantage of the United States.

5.5. Upon receipt of credible and sufficient information that a qualified U.S. contractor has (a) violated U.S. export control law, (b) violated its certification, (c) made a certification in bad faith, or (d) made an omission or misstatement of material fact, the DoD Component shall revoke temporarily the U.S. contractor's qualification. Such revocations having the potential for compromising a U.S. Government investigation may be delayed. Immediately upon such revocation, the DoD Component shall notify the contractor and the OUSDR&E. Such contractor shall be given an opportunity to respond in writing to the information upon which the temporary revocation is based before being disqualified. Any U.S. contractor whose qualification has been revoked temporarily may be reinstated upon presentation of sufficient information showing that the basis for such revocation was in error or has been remedied.

5.6. When the basis for a contractor's temporary revocation cannot be removed within 20 working days, the DoD Component shall recommend to the OUSDR&E that the contractor be disqualified.

5.7. Charges for copying, certifying, and searching records rendered to requesters shall be levied in accordance with DoD Instruction 7230.7 (reference (n)). Normally, only one copy of the same record or document will be provided to each requester. Any release to qualified U.S. contractors of technical data controlled by this Directive shall be accompanied by a notice to the recipient as set forth in enclosure E5.

5.8. Qualified U.S. contractors who receive technical data governed by this Directive may disseminate such data for purposes consistent with their certification without the prior permission of the controlling DoD office or when such dissemination is:

5.8.1. To any foreign recipient for which the data are approved, authorized, or licensed under E.O. 12470 (reference (b)), or the Arms Export Control Act (reference (c)).

5.8.2. To another currently qualified U.S. contractor (as defined in subsection 3.2., above, including existing or potential subcontractors, but only within the scope of the certified legitimate business purpose of such recipient).

5.8.3. To the Departments of State and Commerce, for purposes of applying for appropriate approvals, authorizations, or licenses for export under the Arms Export Control Act (reference (c)) or E.O. 12470 (reference (b)). Any such application shall include a statement that the technical data for which such approval, authorization, or license is sought are controlled by the Department of Defense in accordance with this Directive.

5.8.4. To Congress or any Federal, State, or local governmental agency for regulatory purposes, or otherwise as may be required by law or court order. Any such dissemination shall include a statement that the technical data are controlled by the Department of Defense in accordance with this Directive.

5.9. A qualified U.S. contractor desiring to disseminate technical data subject to this Directive in a manner not permitted expressly by the terms of this Directive shall seek authority to do so from the controlling DoD office.

5.10. Any requester denied technical data, or any qualified U.S. contractor denied permission to re-disseminate such data, pursuant to this Directive, shall be provided promptly a written statement of reasons for that action, and advised of the right to make a written appeal of such determination to a specifically identified appellate authority within the DoD Component. Appeals of denials made under DoD 5400.7-R

(reference (e)) shall be handled in accordance with procedures established therein. Other appeals shall be processed as directed by the OUSDR&E.

5.11. Denials shall cite 10 U.S.C. 140c (reference (a)) as implemented by this Directive, and, in the case of FOIA (reference (i)) denials made in reliance on this statutory authority, 5 U.S.C. 552(b) (3) (reference (i)). Implementing procedures shall provide for resolution of any appeal within 20 working days.

6. RESPONSIBILITIES

6.1. The Under Secretary of Defense for Research and Engineering (USDR&E) shall have overall responsibility for the implementation of this Directive and shall designate an office to:

6.1.1. Administer and monitor compliance with this Directive.

6.1.2. Receive and disseminate notifications of temporary revocation in accordance with subsection 5.5., above.

6.1.3. Receive recommendations for disqualification made in accordance with subsection 5.6., above, and act as initial disqualification authority.

6.1.4. Provide, when necessary, technical assistance to DoD Components in assessing the significance of the military or space application of technical data that may be withheld from public disclosure under this Directive.

6.1.5. Establish procedures to develop, collect, and disseminate certification statements and ensure their sufficiency, accuracy, and periodic renewal, and to make final determinations of qualification.

6.1.6. Ensure that the requirements of this Directive are incorporated into the DoD Federal Acquisition Regulation Supplement (reference (h)) for optional application to contracts involving technical data governed by this Directive.

6.1.7. Develop, in conjunction with the General Counsel, Department of Defense, guidelines for responding to appeals.

6.1.8. Develop procedures to ensure that DoD Components apply consistent criteria in authorizing exceptions under subsection 5.9., above.

6.1.9. *Establish procedures and appropriate mechanisms for the certification of qualified U.S. contractors, pursuant to paragraph 6.1.5., above. DoD Form 2345, "Military Critical Technical Data Agreement" with its associated instructions for completion and submission is established for this purpose.*

6.1.10. Take such other actions that may be required to ensure consistent and appropriate implementation of this Directive within the Department of Defense.

6.2. The Under Secretary of Defense for Policy shall:

6.2.1. Develop and promulgate, as required, policy guidance to DoD Components for implementing this Directive.

6.2.2. Develop procedures with the Departments of State and Commerce to ensure referral of export cases involving technical data governed by this Directive to the Department of Defense.

6.3. The Assistant to the Secretary of Defense for Public Affairs shall:

6.3.1. Monitor the implementation of provisions of this Directive that pertain to DoD 5400.7-R (reference (e)).

6.3.2. Provide such other assistance as may be necessary to ensure compliance with this Directive.

6.4. The General Counsel of the Department of Defense shall:

6.4.1. Assist in carrying out the provisions of this Directive by advising DoD Components with respect to the statutory and regulatory requirements governing the export of technical data.

6.4.2. Advise the USD(A&T) regarding consistent and appropriate implementation of this Directive.

6.5. The Heads of DoD Components shall:

6.5.1. As the delegated authority, have the option to re-delegate the authority to withhold technical data in accordance with this Directive.

6.5.2. Disseminate and withhold from public disclosure technical data subject to this Directive in a manner consistent with the policies and procedures set

forth herein.

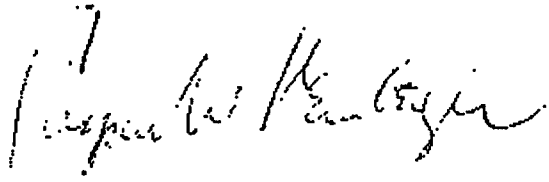
6.5.3. Designate a focal point to (1) ensure implementation of this Directive; (2) identify classes of technical data the release of which is governed by paragraph 5.4.3., above; (3) act on appeals relating to case-by-case denials of technical data; (4) suspend a contractor's qualification pursuant to subsection 5.5., above; (5) receive and evaluate requests for reinstatement of a contractor's qualification; and, when appropriate, (6) recommend disqualification to the OUSDR&E.

6.5.4. Promulgate and effect regulations to implement this Directive within 180 days.

6.5.5. Disseminate technical data governed by this Directive in the manner prescribed herein, to the extent feasible, during the period after which certification procedures have been established under paragraph 6.1.9., above, but before DoD Components have issued implementing regulations under paragraph 6.5.4., above. However, if such dissemination is not feasible, the DoD Component may process requests for such data in accordance with procedures in effect before the promulgation of this Directive.

7. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing documents to the Under Secretary of Defense for (Research and Engineering) within 180 days.



Caspar W. Weinberger
Secretary of Defense

Enclosures - 5

1. References, continued
2. Definitions, continued
3. Pertinent Portions of Export Administration Regulations (EAR)
4. Pertinent Portions of International Traffic in Arms Regulations (ITAR)
5. Notice to Accompany the Dissemination of Export-controlled Technical Data

E1. ENCLOSURE 1

REFERENCES, continued

(d) DoD Instruction 5200.21, "Dissemination of DoD Technical Information," September 27, 1979
(e) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980, authorized by DoD Directive 5400.7, March 24, 1980
(f) Export Administration Regulations
(g) International Traffic in Arms Regulations
(h) DoD Federal Acquisition Regulation Supplement, authorized by DoD Directive 5000.35, "Defense Acquisition Regulatory System," March 8, 1978
(i) Public Law 89-487, "Freedom of Information Act," as amended (5 U.S.C. 552(b)(3) and (4))
(j) Executive Order 12356, "National Security Information," April 2, 1982
(k) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982
(l) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
(m) Militarily Critical Technologies List, October 1984
(n) DoD Instruction 7230.7, "User Charges," June 12, 1979

E2. ENCLOSURE 2

DEFINITIONS, continued

E2.1.1. Controlling DoD Office. The DoD activity that sponsored the work that generated the technical data or received the technical data on behalf of the Department of Defense and therefore has the responsibility for determining the distribution of a document containing such technical data. In the case of joint sponsorship, the controlling office is determined by advance agreement and may be either a party, a group, or a committee representing the interested activities or DoD Components. (The controlling DoD office is identified on each export-controlled document in accordance with DoD Directive 5230.24, reference (l).)

E2.1.2. Critical Technology. Technologies that consist of (a) arrays of design and manufacturing know-how (including technical data); (b) keystone manufacturing, inspection, and test equipment; (c) keystone materials; and (d) goods accompanied by sophisticated operation, application, or maintenance know-how that would make a significant contribution to the military potential of any country or combination of countries and that may prove detrimental to the security of the United States (also referred to as militarily critical technology).

E2.1.3. Other Legitimate Business Purposes. Include:

E2.1.3.1. Providing or seeking to provide equipment or technology to a foreign government with the approval of the U.S. Government (for example, through a licensed direct foreign military sale).

E2.1.3.2. Bidding, or preparing to bid, on a sale of surplus property.

E2.1.3.3. Selling or producing products for the commercial domestic marketplace or for the commercial foreign marketplace, providing that any required export license is obtained.

E2.1.3.4. Engaging in scientific research in a professional capacity.

E2.1.3.5. Acting as a subcontractor to a concern described in (a) through (d) above; or

E2.1.3.6. Selling technical data subject to this Directive in support of DoD contractors or in support of the competitive process for DoD contracts, provided such

sales are limited solely to DoD contractors or potential DoD contractors who also are qualified U.S. contractors and provided such technical data are related to the purpose for which the qualified U.S. contractor is certified, or selling technical data to foreign contractors or governments overseas after receiving the required export license or approval by the U.S. Government.

E2.1.4. Potential DoD Contractor. An individual or organization outside the Department of Defense declared eligible for DoD information services by a sponsoring DoD activity on the basis of participation in one of the following programs:

E2.1.4.1. The Department of the Army Qualitative Requirements Information Program.

E2.1.4.2. The Department of the Navy Industry Cooperative Research and Development Program.

E2.1.4.3. The Department of the Air Force Potential Contractor Program.

E2.1.4.4. The DoD Scientific and Technical Information Program; or

E2.1.4.5. Any similar program in use by other DoD Components.

E2.1.5. Public Disclosure. Making technical data available without restricting its dissemination or use.

E2.1.6. Technical Data with Military or Space Application, or Technical Data. Any blueprints, drawings, plans, instructions, computer software and documentation, or 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 such equipment.

E2.1.7. United States. For the purpose of this Directive, the 50 States, the District of Columbia, and the territories and possessions of the United States.

E3. ENCLOSURE 3

PERTINENT PORTIONS OF EXPORT ADMINISTRATION REGULATIONS (EAR)

The following pertinent section of the EAR is provided for the guidance of DoD personnel in determining the releasability of technical data under the authority of this Directive.

Export Administration Regulations Section 379.3

"General License GTDA: Technical Data Available to All Destinations

"A General License designated GTDA is hereby established authorizing the export to all destinations of technical data described in Section 379.3(a), (b), or (c) below:

"(a) Data Generally Available

"Data that have been made generally available to the public in any form, including -

"(1) Data released orally or visually at open conferences, lectures, trade shows, or other media open to the public; and

"(2) Publications that may be purchased without restrictions at a nominal cost, or obtained without costs, or are readily available at libraries open to the public.

"The term 'nominal cost' as used in Section 379.3(a) (2), above, is intended to reflect realistically only the cost of preparing and distributing the publication and not the intrinsic value of the technical data. If the cost is such as to prevent the technical data from being generally available to the public, General License GTDA would not be applicable.

"(b) Scientific or Educational Data

"(1) Dissemination of information not directly and significantly related to design, production, or utilization in industrial processes, including such dissemination by correspondence, attendance at, or participation in, meetings; or

"(2) Instruction in academic institutions and academic laboratories, excluding information that involves research under contract related directly and significantly to design, production, or utilization in industrial processes.

"(c) Patent Applications

"Data contained in a patent application, prepared wholly from foreign-origin technical data where such application is being sent to the foreign inventor to be executed and returned to the United States for subsequent filing in the U.S. Patent and Trademark Office. (No validated export license from the Office of Export Administration is required for data contained in a patent application, or an amendment, modification, supplement, or division thereof for filing in a foreign country in accordance with the regulations of the Patent and Trademark Office 37 CFR Part 5. See Section 370.10(j).)"

E4. ENCLOSURE 4

PERTINENT PORTIONS OF INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR)

The following pertinent section of the ITAR is provided for the guidance of DoD personnel in determining the releasability of technical data under the authority of this Directive.

International Traffic in Arms Regulations Section 125.11 "General Exemptions

"(a) Except as provided in Section 126.01, district directors of customs and postal authorities are authorized to permit the export without a license of unclassified technical data as follows:

"(1) If it is in published[4] form and subject to public dissemination by being:

"(i) Sold at newsstands and bookstores;

"(ii) Available by subscription or purchase without restrictions to any person or available without cost to any person;

"(iii) Granted second class mailing privileges by the U.S. Government; or,

"(iv) Freely available at public libraries.

"(2) If it has been approved for public release by any U.S. Government Department or Agency having authority to classify information or material under Executive Order [12356], as amended, and other applicable Executive Orders, and does not disclose the details of design, production, or manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List.

---

4 "The burden for obtaining appropriate U.S. Government approval for the publication of technical data falling within the definition in 125.01, including such data as may be developed under other than U.S. Government contract, is on the person or company seeking publication.

"(3) If the export is in furtherance of a manufacturing license or technical assistant agreement approved by the Department of State in accordance with Part 124 of this subchapter.

"(4) If the export is in furtherance of a contract with an Agency of the U.S. Government or a contract between an Agency of the U.S. Government and foreign persons, provided the contract calls for the export of relevant unclassified technical data, and such data are being exported only by the prime contractor. Such data shall not disclose the details of development, engineering, design, production, or manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List. (This exemption does not permit the prime contractor to enter into subsidiary technical assistance or manufacturing license agreements, or any arrangement which calls for the exportation of technical data without compliance with Part 124 of this subchapter.)

"(5) If it relates to firearms not in excess of caliber .50 and ammunition for such weapons, except technical data containing advanced designs, processes, and manufacturing techniques.

"(6) If it consists of technical data, other than design, development, or production information relating to equipment, the export of which has been previously authorized to the same recipient.

"(7) If it consists of operations, maintenance and training manuals, and aids relating to equipment, the export of which has been authorized to the same recipient.[5]

"(8) If it consists of additional copies of technical data previously approved for export to the same recipient; or if it consists of revised copies of technical data, provided it pertains to the identical Munitions List article, and the revisions are solely editorial and do not add to the content of technology previously approved for export to the same recipient.

"(9) If it consists solely of technical data being reexported to the original source of import.

---

5 "Not applicable to technical data relating to Category VI(d) and Category XVI.

"(10) If the export is by the prime contractor in direct support and within the technical and/or product limitations of a 'U.S. Government approved project' and the prime contractor so certifies. The Office of Munitions Control, Department of State, will verify, upon request, those projects which are 'U.S. Government approved,' and accord an exemption to the applicant who applies for such verification and exemption, where appropriate, under this subparagraph.[6]

"(11) If the export is solely for the use of American citizen employees of U.S. firms provided the U.S. firm certifies its overseas employee is a U.S. citizen and has a 'need to know.'[7]

"(12) If the export is directly related to classified information, the export of which has been previously authorized to the same recipient, and does not disclose the details of design, production, or manufacture of any arms, ammunition, or implements of war on the U.S. Munitions List.

"(b) Plant visits. Except as restricted by the provisions of section 126.01 of this subchapter:

"(1) No license shall be required for the oral and visual disclosure of unclassified technical data during the course of a plant visit by foreign nationals provided the data [are] disclosed in connection with a classified plant visit or the visit has the approval of a U.S. Government Agency having authority for the classification of information or material under Executive Order [12356], as amended, and other applicable Executive Orders, and the requirements of section V, paragraph [41(d)] of the Industrial Security Manual are met.

---

6 "Classified information may also be transmitted in direct support of and within the technical and/or product limitation of such verified U.S. Government approved projects without prior department of State approval provided the U.S. party so certifies and complies with the requirements of the Department of Defense Industrial Security Manual relating to the transmission of such classified information (and any other requirements of cognizant U.S. Government departments or agencies).

7 "Classified information may also be exported to such certified American citizen employees without prior Department of State approval provided the U.S. party complies with the requirements of the Department of Defense Industrial Security Manual relating to the transmission of such classified information (and any other requirements of cognizant U.S. Government departments or agencies). Such technical data or information (classified or unclassified) shall not be released by oral, visual, or documentary means to any foreign person.

"(2) No license shall be required for the documentary disclosure of unclassified technical data during the course of a plant visit by foreign nationals provided the document does not contain technical data as defined in Section 125.01 in excess of that released orally or visually during the visit, is within the terms of the approved visit request, and the person in the United States assures that the technical data will not be used, adapted for use, or disclosed to others for the purpose of manufacture or production without the prior approval of the Department of State in accordance with Part 124 of this subchapter.

"(3) No Department of State approval is required for the disclosure of oral and visual classified information during the course of a plant visit by foreign nationals provided the visit has been approved by the cognizant U.S. Defense Agency and the requirements of section V, paragraph [41(d)] of the Defense Industrial Security Manual are met."

E5. ENCLOSURE 5

NOTICE TO ACCOMPANY THE DISSEMINATION OF EXPORT-CONTROLLED TECHNICAL DATA

E5.1.1. Export of information contained herein, which includes, in some circumstances, release to foreign nationals within the United States, without first obtaining approval or license from the Department of State for items controlled by the International Traffic in Arms Regulations (ITAR), or the Department of Commerce for items controlled by the Export Administration Regulations (EAR), may constitute a violation of law.

E5.1.2. Under 22 U.S.C. 2778 the penalty for unlawful export of items or information controlled under the ITAR is up to 2 years imprisonment, or a fine of $100,000, or both. Under 50 U.S.C., Appendix 2410, the penalty for unlawful export of items or information controlled under the EAR is a fine of up to $1,000,000, or five times the value of the exports, whichever is greater; or for an individual, imprisonment of up to 10 years, or a fine of up to $250,000, or both.

E5.1.3. In accordance with your certification that establishes you as a "qualified U.S. contractor," unauthorized dissemination of this information is prohibited and may result in disqualification as a qualified U.S. contractor, and may be considered in determining your eligibility for future contracts with the Department of Defense.

E5.1.4. The U.S. Government assumes no liability for direct patent infringement, or contributory patent infringement or misuse of technical data.

E5.1.5. The U.S. Government does not warrant the adequacy, accuracy, currency, or completeness of the technical data.

E5.1.6. The U.S. Government assumes no liability for loss, damage, or injury resulting from manufacture or use for any purpose of any product, article, system, or material involving reliance upon any or all technical data furnished in response to the request for technical data.

E5.1.7. If the technical data furnished by the Government will be used for commercial manufacturing or other profit potential, a license for such use may be necessary. Any payments made in support of the request for data do not include or involve any license rights.

E5.1.8. A copy of this notice shall be provided with any partial or complete reproduction of these data that are provided to qualified U.S. contractors.

This Page Intentionally Left Blank

DoDD 5400.7

This Page Intentionally Left Blank

Department of Defense
DIRECTIVE

NUMBER 5400.7
September 29, 1997

ASD(PA)

SUBJECT: DoD Freedom of Information Act (FOIA) Program

References: (a) DoD Directive 5400.7, "DoD Freedom of Information Act Program," September 9, 1997 (hereby canceled)
(b) Section 552 of title 5, United States Code, as amended, "Freedom of Information Act"
(c) DoD 5025.1-M, "DoD Directives System Procedures," August 1994, authorized by DoD Directive 5025.1, June 24, 1994
(d) DoD 5400.7-R, "DoD Freedom of Information Act Program," May 22, 1997, authorized by this Directive
(e) through (i), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policies and responsibilities for the implementation of the DoD FOIA Program under reference (b).

1.2. Continues to authorize, consistent with reference (c), the publication of reference (d), the single DoD Regulation on the FOIA Program.

1.3. Continues to delegate authorities and responsibilities for the effective administration of the FOIA program.

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant

Commands, the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. National Security Agency/Central Security Service records are subject to this Directive unless the records are exempt under Section 6 of Pub. L. 86-36 (1959), codified at Section 402 of 50 U.S.C. note (reference (e)). The records of the Defense Intelligence Agency, National Reconnaissance Office, and the National Imagery and Mapping Agency are also subject to this Directive unless the records are exempt under Section 424 of 10 U.S.C. (reference (f)).

3. POLICY

It is DoD policy to:

3.1. Promote public trust by making the maximum amount of information available to the public, in both hard copy and electronic formats, on the operation and activities of the Department of Defense, consistent with DoD responsibility to ensure national security.

3.2. Allow a requester to obtain agency records from the Department of Defense that are available through other public information services without invoking the FOIA.

3.3. Make available, under the procedures established by DoD 5400.7-R (reference (d)), those agency records that are requested by a member of the general public who explicitly or implicitly cites the FOIA.

3.4. Answer promptly all other requests for information, agency records, objects, and articles under established procedures and practices.

3.5. Release agency records to the public unless those records are exempt from mandatory disclosure as outlined in Section 552 of 5 U.S.C. (reference (b)). Make discretionary disclosures of exempt records or information whenever disclosure would not forseeably harm an interest protected by a FOIA exemption.

3.6. Process requests by individuals for access to records about themselves contained in a Privacy Act system of records under procedures set forth in DoD 5400.11-R (reference (g)), and procedures outlined in this Directive as amplified by reference (d).

4. RESPONSIBILITIES

4.1. The Assistant Secretary of Defense for Public Affairs shall:

4.1.1. Direct and administer the DoD FOIA Program to ensure compliance with policies and procedures that govern the administration of the program.

4.1.2. Issue a DoD FOIA regulation and other discretionary instructions and guidance to ensure timely and reasonably uniform implementation of the FOIA in the Department of Defense.

4.1.3. Internally administer the FOIA Program for OSD, the Chairman of the Joint Chiefs of Staff and, as an exception to DoD Directive 5100.3 (reference (h)), the Combatant Commands.

4.1.4. As the designee of the Secretary of Defense, serve as the sole appellate authority for appeals to decisions of respective Initial Denial Authorities within OSD, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, and the DoD Field Activities.

4.2. The General Counsel of the Department of Defense shall provide uniformity in the legal interpretation of this Directive.

4.3. The Heads of the DoD Components shall:

4.3.1. Publish in the "FEDERAL REGISTER" any instructions necessary for the internal administration of this Directive within a DoD Component that are not prescribed by this Directive or by other issuances of the Assistant Secretary of Defense (Public Affairs). For the guidance of the public, the information specified in Section 552(a)(1) of 5 U.S.C. (reference (b)) shall be published in accordance with DoD Directive 5400.9 (reference (i)).

4.3.2. Conduct training on the provisions of this Directive, reference (b), and DoD 5400.7-R (reference (d)) for officials and employees who implement the FOIA.

4.3.3. Submit the report prescribed in Chapter 7 of reference (d).

4.3.4. Make available for public inspection and copying in an appropriate facility or facilities, in accordance with rules published in the "FEDERAL

REGISTER," the records specified in Section 552(a)(2) of reference (b), unless such records are published and copies are offered for sale. These records shall be made available to the public in hard copy, by computer telecommunications, or other electronic means.

4.3.5. Maintain and make available for public inspection and copying current indices of all (a)(2) records as required by section 552(a)(2) of reference (b).

5. INFORMATION REQUIREMENTS

The reporting requirements in Chapter 7 of reference (d) have been assigned Report Control Symbol DD-PA(A)1365.

6. EFFECTIVE DATE

This Directive is effective immediately.

John J. Hamre
Deputy Secretary of Defense

Enclosures - 1
1. References

E1. ENCLOSURE 1

REFERENCES, continued

(e) Section 6 of Public Law 86-36, codified at Section 402 of title 50, United States Code, note, "National Security Agency Act of 1959"

(f) Section 424 of title 10, United States Code, "Disclosure of Organizational and Personnel Information: Exemption for Defense Intelligence Agency, National Reconnaissance Office and National Imagery and Mapping Agency"

(g) DoD 5400.11-R, "Department of Defense Privacy Program," August 31, 1983, authorized by DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982

(h) DoD Directive 5100.3, "Support of the Headquarters of Unified, Specified and Subordinate Commands," November 1, 1988

(i) DoD Directive 5400.9, "Publication of Proposed and Adopted Regulations Affecting the Public," December 23, 1974

This Page Intentionally Left Blank

DoDD 5400.11

This Page Intentionally Left Blank

Department of Defense
DIRECTIVE

NUMBER 5400.11
December 13, 1999

DA&M

SUBJECT: DoD Privacy Program

References: (a) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982 (hereby canceled)
(b) Section 552a and Chapter 8 of title 5, United States Code
(c) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," February 8, 1996
(d) DoD 5400.11-R, "Department of Defense Privacy Program," August 1983, authorized by this Directive
(e) through (i), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policies and responsibilities of the DoD Privacy Program under Section 552a of reference (b), and under reference (c).

1.2. Authorizes the Defense Privacy Board, the Defense Privacy Board Legal Committee and the Defense Data Integrity Board.

1.3. Continues to authorize the publication of reference (d).

1.4. Continues to delegate authorities and responsibilities for the effective administration of the DoD Privacy Program.

2. APPLICABILITY

This Directive:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Uniformed Services University of the Health Sciences, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Shall be made applicable to DoD contractors who are operating a system of records on behalf of a DoD Component, to include any of the activities, such as collecting and disseminating records, associated with maintaining a system of records.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. The personal privacy of an individual shall be respected and protected.

4.2. Personal information shall be collected, maintained, used or disclosed to ensure that:

4.2.1. It shall be relevant and necessary to accomplish a lawful DoD purpose required to be accomplished by statute or Executive order;

4.2.2. It shall be collected to the greatest extent practicable directly from the individual;

4.2.3. The individual shall be informed as to why the information is being collected, the authority for collection, what uses will be made of it, whether disclosure is mandatory or voluntary, and the consequences of not providing that information;

4.2.4. It shall be relevant, timely, complete and accurate for its intended use; and

4.2.5. Appropriate administrative, technical, and physical safeguards shall be established, based on the media (e.g., paper, electronic, etc.) involved, to ensure the security of the records and to prevent compromise or misuse during storage or transfer.

4.3. No record shall be maintained on how an individual exercises rights guaranteed by the First Amendment to the Constitution, except as follows:

4.3.1. Specifically authorized by statute;

4.3.2. Expressly authorized by the individual on whom the record is maintained; or

4.3.3. When the record is pertinent to and within the scope of an authorized law enforcement activity.

4.4. Notices shall be published in the "Federal Register" and reports shall be submitted to Congress and the Office of Management and Budget, in accordance with, and as required by, Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (c) through (d)), as to the existence and character of any system of records being established or revised by the DoD Components. Information shall not be collected, maintained, used, or disseminated until the required publication/review requirements, as set forth in Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (c) through (d)), are satisfied.

4.5. Individuals shall be permitted, to the extent authorized by Section 552a of reference (b) and reference (d), to:

4.5.1. Determine what records pertaining to them are contained in a system of records;

4.5.2. Gain access to such records and to obtain a copy of those records or a part thereof;

4.5.3. Correct or amend such records on a showing that the records are not accurate, relevant, timely or complete;

4.5.4. Appeal a denial of access or a request for amendment.

4.6. Disclosure of records pertaining to an individual from a system of records shall be prohibited except with the consent of the individual or as otherwise authorized by Section 552a of reference (b), reference (d), and DoD 5400.7-R (reference (e)).

When disclosures are made, the individual shall be permitted, to the extent authorized by Section 552a of reference (b) and reference (d), to seek an accounting of such disclosures from the DoD Component making the release.

4.7. Disclosure of records pertaining to personnel of the National Security Agency, the Defense Intelligence Agency, the National Reconnaissance Office, and the National Imagery and Mapping Agency shall be prohibited to the extent authorized by Pub. L. No. 86-36 (1959) and 10 U.S.C. 424 (references (f) and (g)).

4.8. Computer matching programs between the DoD Components and the Federal, State, or local governmental agencies shall be conducted in accordance with the requirements of Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)).

4.9. DoD personnel and system managers shall conduct themselves, consistent with established rules of conduct (enclosure 3), so that personal information to be stored in a system of records only shall be collected, maintained, used, and disseminated as is authorized by this Directive, Section 552a of reference (b), and reference (d).

5. RESPONSIBILITIES

5.1. The Director of Administration and Management, Office of the Secretary of Defense, shall:

5.1.1. Serve as the Senior Privacy Official for the Department of Defense.

5.1.2. Provide policy guidance for, and coordinate and oversee administration of, the DoD Privacy Program to ensure compliance with policies and procedures in Section 552a of reference (b) and reference (c).

5.1.3. Publish reference (d) and other guidance, to include Defense Privacy Board Advisory Opinions, to ensure timely and uniform implementation of the DoD Privacy Program.

5.1.4. Serve as the Chair to the Defense Privacy Board and the Defense Data Integrity Board (enclosure 4).

5.2. The Director of Washington Headquarters Services shall supervise and oversee the activities of the Defense Privacy Office (enclosure 4).

5.3. The General Counsel of the Department of Defense shall:

5.3.1. Provide advice and assistance on all legal matters arising out of, or incident to, the administration of the DoD Privacy Program.

5.3.2. Review and be the final approval authority on all advisory opinions issued by the Defense Privacy Board or the Defense Privacy Board Legal Committee.

5.3.3. Serve as a member of the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee (enclosure 4).

5.4. The Secretaries of the Military Departments and the Heads of the Other DoD Components shall:

5.4.1. Provide adequate funding and personnel to establish and support an effective DoD Privacy Program, to include the appointment of a senior official to serve as the principal point of contact (POC) for DoD Privacy Program matters.

5.4.2. Establish procedures, as well as rules of conduct, necessary to implement this Directive and DoD 5400.11-R (reference (d)) so as to ensure compliance with the requirements of Section 552a of 5 U.S.C. and OMB Circular A-130 (references (b) and (c)).

5.4.3. Conduct training, consistent with the requirements of reference (d), on the provisions of this Directive, Section 552a of reference (b), and references (c) and (d), for assigned and employed personnel and for those individuals having primary responsibility for implementing the DoD Privacy Program.

5.4.4. Ensure that the DoD Privacy Program periodically shall be reviewed by the Inspectors General or other officials, who shall have specialized knowledge of the DoD Privacy Program.

5.4.5. Submit reports, consistent with the requirements of DoD 5400.11-R (reference (d)), as mandated by Section 552a and Chapter 8 of 5 U.S.C. (reference (b)), OMB Circular A-130 (reference (c)), and DoD Directive 5400.12 (reference (h)), and as otherwise directed by the Defense Privacy Office.

5.5. The Secretaries of the Military Departments shall provide support to the Combatant Commands, as identified in DoD Directive 5100.3 (reference (i)), in the administration of the DoD Privacy Program.

6. INFORMATION REQUIREMENTS

The reporting requirements in paragraph 5.4.5., above, are assigned Report Control Symbol DD-DA&M(A)1379.

7. EFFECTIVE DATE

This Directive is effective immediately.

John J. Hamre
Deputy Secretary of Defense

Enclosures - 4

E1. References, continued
E2. Definitions
E3. Rules of Conduct
E4. Privacy Boards and Office

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998, authorized by DoD Directive 5400.7, September 29, 1997

(f) Public Law 86-36, "National Security Agency-Officers and Employees," May 29, 1959

(g) Section 424 of title 10, United States Code

(h) DoD Directive 5400.12, "Obtaining Information from Financial Institutions," February 6, 1980

(i) DoD Directive 5100.3, "Support of Headquarters of the Unified, Specified, and Subordinate Joint Commands, " November 1, 1988

E2. ENCLOSURE 2

DEFINITIONS

The Following terms are used in the Directive:

E2.1.1. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals."

E2.1.2. Personal Information. Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., a social security number, age, military rank, civilian grade, marital status, race, salary, home/office phone numbers, etc.

E2.1.3. Record. Any item, collection, or grouping of information, whatever the storage media (e.g., paper, electronic, etc.), about an individual that is maintained by a DoD Component, including but not limited to, his or her education, financial transactions, medical history, criminal or employment history and that contains his or her name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

E2.1.4. System Manager. The DoD Component official who is responsible for the operation and management of a system of records.

E2.1.5. System of Records. A group of records under the control of a DoD Component from which personal information is retrieved by the individual's name or by some identifying number, symbol, or other identifying particular assigned to an individual.

E3. ENCLOSURE 3

RULES OF CONDUCT

E3.1. DoD PERSONNEL SHALL:

E3.1.1. Take such actions, as considered appropriate, to ensure that personal information contained in a system of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information shall be preserved.

E3.1.2. Not disclose any personal information contained in any system of records except as authorized by DoD 5400.11-R (reference (d)) or other applicable law or regulation. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.

E3.1.3. Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized by this Directive to the applicable Privacy POC for his or her DoD Component.

E3.2. DoD SYSTEM MANAGERS FOR EACH SYSTEM OF RECORDS SHALL:

E3.2.1. Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities for protecting personal information being collected and maintained under the DoD Privacy Program.

E3.2.2. Prepare promptly any required new, amended, or altered system notices for the system of records and submit them through their DoD Component Privacy POC to the Defense Privacy Office for publication in the "Federal Register."

E3.2.3. Not maintain any official files on individuals which are retrieved by name or other personal identifier without first ensuring that a notice for the system of records shall have been published in the "Federal Register." Any official who willfully maintains a system of records without meeting the publication requirements, as prescribed by Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)), is subject to possible criminal penalties and/or administrative sanctions.

E4. ENCLOSURE 4

PRIVACY BOARDS AND OFFICE COMPOSITION AND RESPONSIBILITIES

E4.1. THE DEFENSE PRIVACY BOARD

E4.1.1. Membership. The Board shall consist of the Director of Administration and Management, OSD(DA&M), who shall serve as the Chair; the Director of the Defense Privacy Office, Washington Headquarters Services (WHS), who shall serve as the Executive Secretary and as a member; the representatives designated by the Secretaries of the Military Departments; and the following officials or their designees: the Deputy Under Secretary of Defense for Program Integration (DUSD(PI)); the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)); the Director, Freedom of Information and Security Review, WHS; the General Counsel of the Department of Defense (GC, DoD); and the Director for Information Operations and Reports, WHS (DIO&R). The designees also may be the principal POC for the DoD Component for privacy matters.

E4.1.2. Responsibilities

E4.1.2.1. The Board shall have oversight responsibility for implementation of the DoD Privacy Program. It shall ensure that the policies, practices, and procedures of that Program are premised on the requirements of Section 552a of 5 U.S.C. and OMB Circular A-130 (references (b) and (c)), as well as other pertinent authority, and that the Privacy Programs of the DoD Component are consistent with, and in furtherance of, the DoD Privacy Program.

E4.1.2.2. The Board shall serve as the primary DoD policy forum for matters involving the DoD Privacy Program, meeting as necessary, to address issues of common concern so as to ensure that uniform and consistent policy shall be adopted and followed by the DoD Components. The Board shall issue advisory opinions as necessary on the DoD Privacy Program so as to promote uniform and consistent application of Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)).

E4.1.2.3. Perform such other duties as determined by the Chair or the Board.

E4.2. THE DEFENSE DATA INTEGRITY BOARD

E4.2.1. Membership. The Board shall consist of the DA&M, OSD, who shall serve as the Chair; the Director of the Defense Privacy Office, WHS, who shall serve as the Executive Secretary; and the following officials or their designees: the representatives designated by the Secretaries of the Military Departments; the DUSD(PI); the ASD(C3I); the GC, DoD; the IG, DoD; the DIO&R(WHS); and the Director, Defense Manpower Data Center. The designees also may be the principal POC for the DoD Component for privacy matters.

E4.2.2. Responsibilities

E4.2.2.1. The Board shall oversee and coordinate, consistent with the requirements of Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through(d)), all computer matching programs involving personal records contained in system of records maintained by the DoD Components.

E4.2.2.2. The Board shall review and approve all computer matching agreements between the Department of Defense and the other Federal, State or local governmental agencies, as well as memoranda of understanding when the match is internal to the Department of Defense, to ensure that, under Section 552a of reference (b) and references (c) and (d), appropriate procedural and due process requirements shall have been established before engaging in computer matching activities.

E4.3. THE DEFENSE PRIVACY BOARD LEGAL COMMITTEE

E4.3.1. Membership. The Committee shall consist of the Director, Defense Privacy Office, WHS, who shall serve as the Chair and the Executive Secretary; the GC, DoD, or designee; and civilian and/or military counsel from each of the DoD Components. The General Counsels (GCs) and The Judge Advocates General of the Military Departments shall determine who shall provide representation for their respective Department to the Committee. That does not preclude representation from each office. The GCs of the other DoD Components shall provide legal representation to the Committee. Other DoD civilian or military counsel may be appointed by the Executive Secretary, after coordination with the DoD Component concerned, to serve on the Committee on those occasions when specialized knowledge or expertise shall be required.

E4.3.2. Responsibilities

E4.3.2.1. The Committee shall serve as the primary legal forum for addressing and resolving all legal issues arising out of or incident to the operation of the DoD Privacy Program.

E4.3.2.2. The Committee shall consider legal questions regarding the applicability of Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)) and questions arising out of or as a result of other statutory and regulatory authority, to include the impact of judicial decisions, on the DoD Privacy Program. The Committee shall provide advisory opinions to the Defense Privacy Board and, on request, to the DoD Components.

E4.4. THE DEFENSE PRIVACY OFFICE

E4.4.1. Membership. It shall consist of a Director and a staff. The Director also shall serve as the Executive Secretary and a member of the Defense Privacy Board; as the Executive Secretary to the Defense Data Integrity Board; and as the Chair and the Executive Secretary to the Defense Privacy Board Legal Committee.

E4.4.2. Responsibilities

E4.4.2.1. Manage activities in support of the Privacy Program oversight responsibilities of the DA&M.

E4.4.2.2. Provide operational and administrative support to the Defense Privacy Board, the Defense Data Integrity Board, and the Defense Privacy Board Legal Committee.

E4.4.2.3. Direct the day-to-day activities of the DoD Privacy Program.

E4.4.2.4. Provide guidance and assistance to the DoD Components in their implementation and execution of the DoD Privacy Program.

E4.4.2.5. Review proposed new, altered, and amended systems of records, to include submission of required notices for publication in the "Federal Register" and, when required, providing advance notification to the Office of Management and Budget (OMB) and the Congress, consistent with Section 552a of 5 U.S.C., OMB Circular A-130, and DoD 5400.11-R (references (b) through (d)).

E4.4.2.6. Review proposed DoD Component privacy rulemaking, to include submission of the rule to the Office of the Federal Register for publication and providing to the OMB and the Congress reports, consistent with Section 552a of reference (b) and references (c) and (d), and to the Office of the Comptroller General of the United States, consistent with Chapter 8 of reference (b).

E4.4.2.7. Develop, coordinate, and maintain all DoD computer matching agreements, to include submission of required match notices for publication in the "Federal Register" and advance notification to the OMB and the Congress of the proposed matches, consistent with Section 552a of reference (b) and references (c) and (d).

E4.4.2.8. Provide advice and support to the DoD Components to ensure that:

E4.4.2.8.1. All information requirements developed to collect or maintain personal data conform to DoD Privacy Program standards;

E4.4.2.8.2. Appropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic on non-electronic means; and

E4.4.2.8.3. Specific procedures and safeguards shall be developed and implemented when personal data is collected and maintained for research purposes.

E4.4.2.9. Serve as the principal POC for coordination of privacy and related matters with the OMB and other Federal, State, and local governmental agencies.

E4.4.2.10. Compile and submit the "Biennial 'Privacy Act' Report" and the "Biennial Matching Activity Report" to the OMB as required by OMB Circular A-130 and DoD 5400.11-R (references (c) and (d)).

E4.4.2.11. Update and maintain this Directive and reference (d).

DoDD 8910.1

This Page Intentionally Left Blank

Department of Defense

DIRECTIVE

NUMBER 8910.1

June 11, 1993

ASD(C3I)

SUBJECT: Management and Control of Information Requirements

References: (a) DoD Directive 7750.5, subject as above, August 7, 1986 (hereby canceled)
(b) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992
(c) Public Law 96-511, "The Paperwork Reduction Act of 1980," December 11, 1980, as amended (44 U.S.C. 350 et seq.)
(d) DoD 8910.1-M, "DoD Procedures for Management of Information Requirements," November 1986, authorized by this Directive
(e) through (q), see enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Administratively renumbers and reissues reference (a).

1.2. Establishes policy and assigns responsibilities for the management and control of information requirements and implements those policies in references (b) and (c) on the licensing of reporting requirements internal and external to the Department of Defense and the development of an information collection budget.

1.3. Continues to authorize publication of DoD 7750.5-M, hereby changed to DoD 8910.1-M (reference (d)), and DoD 7750.5-L, hereby changed to DoD 8910.1-L (reference (e)), in accordance with DoD 5025.1-M (reference (f)).

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments (including the National Guard and Reserve components), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2.2. Applies to existing, revised, and new information requirements (internal DoD, inter-Agency, and public reporting requirements) and the systems and processes necessary to support them. All information and reporting systems and all techniques (electronic and manual) for collecting, recording, maintaining, and disseminating information for all functional areas are included under its provisions unless specifically exempted by reference (c).

2.3. Encompasses the information requirements developed in support of all management functions, unless excluded in reference (d) and includes information collected to satisfy statutory, congressional, and other inter-Agency imposed information requirements; the collection of information from sources external to the Federal Government; and information collected internally within the Department of Defense.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

4.1. Ensuring that sufficient information is available to achieve military effectiveness and management efficiency is a basic command and management responsibility. As a fundamental policy, however, the burden associated with the collection and reporting of this information must be controlled and minimized. The management of reports internally prescribed by the DoD Component must include provision for setting annual goals, consistent with critical mission needs, to reduce the number or frequency of reports.

4.2. The central ingredient in information management is the user's responsibility and accountability for ensuring that information requirements are valid, accurate, and essential to the mission of the user's organization.

4.2.1. Information requirements should be examined to avoid both duplication and unnecessary generation of data. Because the creation or collection of information requires the allocation of scarce resources, the user must first ascertain that the required data are not already available from other sources.

4.2.2. Statistical sampling techniques and information technology should be emphasized as approaches for minimizing reporting workloads.

4.2.3. In the development and operational life cycle of an automated information system, care shall be taken to ensure that information needs are clearly identified and that reports to be generated by the automated system represent cost-effective use of resources, as required by DoD Directive 8120.1 (reference (g)).

4.3. Information collected from the public (individuals, businesses, and other private institutions) and State and local governments shall also be minimized, accounted for, and controlled. Section 1320 of 5 CFR (reference (h)) directs that public information collections be submitted to the Office of Management and Budget (OMB) for approval, and that an annual information collection budget of burden hours be developed and submitted to the OMB.

4.4. To ensure optimum effectiveness and economy in the development of information requirements, the following guidance shall be applied:

4.4.1. Each new or revised information requirement shall be subjected to a cost analysis. An estimate or actual cost of obtaining the information shall be developed by the requester in accordance with DoD 8910.1-M (reference (d)). A full cost-benefit analysis shall be required for all information collections and systems that are considered to be major by a senior information resources management (IRM) official or representative.

4.4.2. Each item of data in the information requirement shall be evaluated and screened against data in existing information collections to determine whether such information can satisfy the requirement. Information requirements shall be designed to meet only essential needs and be in the minimal frequency feasible, with reasonable due dates. The number of copies to be prepared shall be held to a minimum. Repetitive one-time information requirements may not be imposed when the need for a recurring information requirement is indicated.

4.4.3. Information requirements shall comply with existing standard data elements and codes published in DoD 5000.12-M (reference (i)). If required data

elements and codes do not exist, they shall be standardized, when appropriate, consistent with DoD Directive 8320.1 (reference (j)).

4.4.4. Internal DoD information requirements shall be approved and symbolized; i.e., assigned an information requirement control symbol at the organizational Component level generating the requirement.

4.4.5. Information requirements that have not been properly approved and symbolized shall not be honored. The office requesting the data shall be notified that an information requirement control symbol must be obtained before the data can be collected.

4.4.6. Information requirements that involve the collection of personal information on individuals require special handling under DoD Directive 5400.11 (reference (k)). Information or data included in the proposed information requirement shall be accessible to the public, only as prescribed by DoD Directive 5400.7 (reference (l)).

4.4.7. On an individual case-by-case basis, special one-time, high priority, or time-urgent requirements may be approved and symbolized without being subjected to in-depth review and analysis, provided a statement of urgency is included with the request for approval document. It will be the responsibility of the requester to complete the request for approval document retroactively, including the appropriate justification and cost estimates.

4.5. To ensure that ongoing information requirements are still valid and adequate, users shall perform assessments of their ongoing information requirements no less frequently than every 3 years. Actions shall be taken to accomplish modifications, cancellations, or new initiatives identified during the review. The DoD Components should consider the assignment of expiration dates to reports as a means of distributing the workload of relicensing reports.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, as the DoD senior official responsible for implementing Pub.L. No. 96-511 (1980) (reference (c)), shall, consistent with the guidance prescribed by the OMB:

5.1.1. Develop and issue DoD-wide policies for the management, control,

and registration of internal DoD, inter-Agency, and public reporting requirements.

5.1.2. Establish goals, as appropriate, consistent with critical mission needs, for reduction in the number and frequency of OSD-prescribed internal reports.

5.1.3. Oversee accomplishment of all DoD report reduction goals.

5.1.4. Provide policy oversight and monitor the information collection budget.

5.1.5. Approve and publish DoD 8910.1-M (reference (d)), in accordance with DoD 5025.1-M (reference (f)).

5.2. The Assistant Secretary of Defense (Production and Logistics) shall review and administer data requirements acquired by solicitation or contract, and publish and maintain DoD 5010.12-L (reference (m)), in accordance with DoD Instruction 5000.2 (reference (n)).

5.3. The Assistant Secretary of Defense (Force Management and Personnel) shall, before submission to the Director, Washington Headquarters Services (WHS), approve surveys requiring participation of personnel in any DoD Component, other than the sponsoring Component, as prescribed by DoD Instruction 1100.13 (reference (o)).

5.4. The Director, Washington Headquarters Services, shall:

5.4.1. Develop and coordinate DoD 8910.1-M (reference (d)) to provide procedures governing the processing, review, and approval of information requirements (DoD internal, inter-Agency, and public reports).

5.4.2. Establish an OSD information requirements control activity to:

5.4.2.1. Maintain and distribute an index of approved information requirements (DoD 8910.1-L (reference (e))).

5.4.2.2. Maintain the data profiles of all DoD public, inter-Agency, and OSD-prescribed internal reports on an automated locator system. This system should be compatible with the Federal Information Locator System established by Pub. L. No. 96-511(1980) (reference (c)).

5.4.2.3. Serve as the DoD reviewing office and the office of record for inter-Agency information requirements imposed by the Department of Defense or by external agencies, in accordance with the Federal Information Resources Management

Regulation (FIRMR) (reference (p)).

5.4.2.4. Serve as the DoD clearance office and the office of record for DoD public reporting, in accordance with Pub. L. No. 96-511(1980) (reference (c)) and 5 CFR 1320 (reference (h)).

5.4.2.5. Serve as the office of record and approval authority for OSD-prescribed internal information requirements, in accordance with the FIRMR (reference (p)).

5.4.3. Take appropriate action on the results of OSD staff assessments of their ongoing information requirements.

5.5. The Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Directors of the Defense Agencies shall:

5.5.1. Ensure that users justify new information requirements before submission for approval to ensure that the data are not already available from other sources.

5.5.2. Establish an information requirements control activity under their senior IRM official or representative to:

5.5.2.1. Serve as the principal point of contact on the various information requirements programs.

5.5.2.2. Provide for the efficient and effective management and control of information requirements.

5.5.2.3. Process, assign, and cancel internal information requirement control symbols where applicable. Information requirement control symbols assigned by a higher level shall not be assigned a different information requirement control symbol by a lower level organization.

5.5.2.4. Submit their respective information collection budgets to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)).

5.5.2.5. Submit their requests for public and interagency information requirements to the Director, WHS.

5.5.2.6. Maintain an up-to-date index of their approved information requirements.

5.5.3. Respond only to those information requirements that have been symbolized; that is, assigned an information requirement control symbol, an inter-Agency report control number, or an OMB approval number, or exempted, consistent with DoD 8910.1-M (reference (d)).

5.5.4. Maintain cost information consistent with paragraph 4.4.1., above. When appropriate, cost information shall also be maintained at other levels of command.

5.5.5. Establish goals, as appropriate, consistent with critical mission needs, for reduction in the number or frequency of their internally prescribed reports.

5.5.6. Ensure that users assess their ongoing information requirements no less frequently than every 3 years, take appropriate action, and communicate the results of their actions to the information requirements control activity.

5.6. The OSD Principal Staff Assistants shall:

5.6.1. Designate an information management control officer for their respective functional areas.

5.6.2. Submit their information requirement requests to the Director, WHS.

5.6.3. Respond only to those public and inter-Agency information requirements that have valid control numbers.

5.6.4. Submit their respective information collection budgets to the ASD(C3I).

5.6.5. Assess their ongoing information requirements no less frequently than every 3 years and communicate the results of the assessment to the Director, WHS.

6. INFORMATION REQUIREMENTS

The Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, and the Directors of the Defense Agencies are hereby delegated authority to approve, symbolize, or exempt their own prescribed internal information requirements.

7. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. The Heads of the DoD Components shall keep implementing documents to the absolute minimum. Forward one copy of implementing documents to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence within 120 days.

William J. Perry
Deputy Secretary of Defense

Enclosures - 2

1. References
2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD 8910.1 -L, "Listing of Approved Recurring Information Requirements," January 1993, authorized by this Directive
(f) DoD 5025.1-M, "DoD Directives System Procedures," December 1990, authorized by DoD Directive 5025.1, December 23, 1988
(g) DoD Directive 8120.1, "Life Cycle Management (LCM) of Automated Information Systems (AISs)," January 14, 1993
(h) Title 5, Code of Federal Regulations, Section 1320
(i) DoD 5000.12-M, "DoD Manual for Standard Data Elements," July 1989, authorized by DoD Instruction 5000.12, April 27, 1965
(j) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
(k) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
(l) DoD Directive 5400.7, "DoD Freedom of Information Act Program," May 13, 1988
(m) DoD 5010.12-L, "Acquisition Management Systems and Data Requirements Control List," October 1992, authorized by DoD Instruction 5000.2, February 23, 1991
(n) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991
(o) DoD Instruction 1100.13, "Surveys of Department of Defense Personnel," November 9, 1978
(p) Federal Information Resources Management Regulation (FIRMR), Part 201-9, April 29, 1991 (Title 41, Code of Federal Regulations, Chapter 201)
(q) Office of Management and Budget (OMB) Circular A-130, "Management of Information Resources," December 12, 1985

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Information. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microform, or magnetic tape. (See OMB Circular A-130, reference (q).)

E2.1.2. Information Collection Budget. An annual comprehensive budget of burden hours for all collections of information from the public to be conducted or sponsored by a Federal Agency in the succeeding 12 months.

E2.1.3. Information Collection Request. A written report form, application form, survey, schedule, questionnaire, reporting or record keeping requirement, or other similar method calling for the collection of information.

E2.1.4. Information Requirement. The functional area expression of need for data or information to carry out specified and authorized functions or management purposes that require the establishment or maintenance of forms or formats, or reporting or record keeping systems, whether manual or automated.

E2.1.5. Information Requirements Assessment. The analysis of ongoing information requirements to ascertain the need for the information, the cycle of reporting, the timeliness of the requirement, the accuracy of the information, and the cost-effectiveness of the requirement.

E2.1.6. Information Resources Management (IRM). The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by Agencies. The term includes the management of information and related resources, such as Federal information processing resources. (See Pub. L. No. 96-511(1980), reference (c).)

E2.1.7. OSD Principal Staff Assistants. The Under Secretaries of Defense; the Assistant Secretaries of Defense; the General Counsel of the Department of Defense; the Inspector General of the Department of Defense; the Comptroller of the Department of Defense; the Assistants to the Secretary of Defense; and the OSD Directors, or equivalents, who report directly to the Secretary or the Deputy Secretary

of Defense (DoD 5025.1-M, reference (f)).

E2.1.8. Senior IRM Official or Representative. The term is defined to include the single official for IRM designated under reference (c) and those representatives in the Defense Agencies, designated by their Heads, as responsible for oversight of Agency information matters.

E2.1.9. Surveys of Persons. Systematic data collections, using personal or telephonic interviews, or self-administered questionnaires, from a sample of 10 or more persons as individuals or representatives of Agencies that elicit attitudes, opinions, behavior, and related demographic, social, and economic data to identical questions that are to be used for statistical compilations for research and/or policy assessment purposes.

This Page Intentionally Left Blank

EO 12958

This Page Intentionally Left Blank

federal register

Thursday
April 20, 1995

Part IV

The President

Executive Order 12958—Classified National Security Information

This Page Intentionally Left Blank

Table of Contents

		Page
PREAMBLE		1
PART 1	ORIGINAL CLASSIFICATION	
1.1	Definitions	1
1.2	Classification Standards	2
1.3	Classification Levels	3
1.4	Classification Authority	3
1.5	Classification Categories	4
1.6	Duration of Classification	4
1.7	Identification and Markings	5
1.8	Classification Prohibitions and Limitations	6
1.9	Classification Challenges	7
PART 2	DERIVATIVE CLASSIFICATION	
2.1	Definitions	7
2.2	Use of Derivative Classification	8
2.3	Classification Guides	8
PART 3	DECLASSIFICATION AND DOWNGRADING	
3.1	Definitions	8
3.2	Authority for Declassification	9
3.3	Transferred Information	10
3.4	Automatic Declassification	10
3.5	Systematic Declassification Review	12
3.6	Mandatory Declassification Review	13
3.7	Processing Requests and Reviews	14
3.8	Declassification Database	14
PART 4	SAFEGUARDING	
4.1	Definitions	14
4.2	General Restrictions on Access	15
4.3	Distribution Controls	16
4.4	Special Access Programs	16
4.5	Access by Historical Researchers and Former Presdential Appointees	17
PART 5	IMPLEMENTATION AND REVIEW	
5.1	Definitions	18
5.2	Program Direction	18

5.3 Information Security Oversight Office 18
5.4 Interagency Security Classification Appeals Panel 19
5.5 Information Security Policy Advisory Council 20
5.6 General Responsibilities 21
5.7 Sanctions 22

PART 6 GENERAL PROVISIONS

6.1 General Provisions 23
6.2 Effective Date 23

Federal Register
Vol. 60, No. 76
Thursday, April 20, 1995

Presidential Documents

Title 3—

The President

Executive Order 12958 of April 17, 1995

Classified National Security Information

This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation's progress depends on the free flow of information. Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Protecting information critical to our Nation's security remains a priority. In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.

NOW, THEREFORE, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

PART 1—ORIGINAL CLASSIFICATION

Section 1.1. *Definitions.* For purposes of this order:

(a) "National security" means the national defense or foreign relations of the United States.

(b) "Information" means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, that is owned by, produced by or for, or is under the control of the United States Government. "Control" means the authority of the agency that originates information, or its successor in function, to regulate access to the information.

(c) "Classified national security information" (hereafter "classified information") means information that has been determined pursuant to this order or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

(d) "Foreign Government Information" means:

(1) information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence;

(2) information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; or

(3) information received and treated as "Foreign Government Information" under the terms of a predecessor order.

(e) "Classification" means the act or process by which information is determined to be classified information.

(f) "Original classification" means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

(g) "Original classification authority" means an individual authorized in writing, either by the President, or by agency heads or other officials designated by the President, to classify information in the first instance.

(h) "Unauthorized disclosure" means a communication or physical transfer of classified information to an unauthorized recipient.

(i) "Agency" means any "Executive agency," as defined in 5 U.S.C. 105, and any other entity within the executive branch that comes into the possession of classified information.

(j) "Senior agency official" means the official designated by the agency head under section 5.6(c) of this order to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

(k) "Confidential source" means any individual or organization that has provided, or that may reasonably be expected to provide, information to the United States on matters pertaining to the national security with the expectation that the information or relationship, or both, are to be held in confidence.

(l) "Damage to the national security" means harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information.

Sec. 1.2. *Classification Standards.* (a) Information may be originally classified under the terms of this order only if all of the following conditions are met:

(1) an original classification authority is classifying the information;
(2) the information is owned by, produced by or for, or is under the control of the United States Government;
(3) the information falls within one or more of the categories of information listed in section 1.5 of this order; and
(4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security and the original classification authority is able to identify or describe the damage.

(b) If there is significant doubt about the need to classify information, it shall not be classified. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or
(2) create any substantive or procedural rights subject to judicial review.

(c) Classified information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information.

Sec. 1.3. *Classification Levels.* (a) Information may be classified at one of the following three levels:

(1) "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
(2) "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
(3) "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(b) Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.

(c) If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.

Sec. 1.4. *Classification Authority.* (a) The authority to classify information originally may be exercised only by:

(1) the President;

(2) agency heads and officials designated by the President in the **Federal Register**; or

(3) United States Government officials delegated this authority pursuant to paragraph (c), below.

(b) Officials authorized to classify information at a specified level are also authorized to classify information at a lower level.

(c) Delegation of original classification authority.

(1) Delegations of original classification authority shall be limited to the minimum required to administer this order. Agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority.

(2) "Top Secret" original classification authority may be delegated only by the President or by an agency head or official designated pursuant to paragraph (a)(2), above.

(3) "Secret" or "Confidential" original classification authority may be delegated only by the President; an agency head or official designated pursuant to paragraph (a)(2), above; or the senior agency official, provided that official has been delegated "Top Secret" original classification authority by the agency head.

(4) Each delegation of original classification authority shall be in writing and the authority shall not be redelegated except as provided in this order. Each delegation shall identify the official by name or position title.

(d) Original classification authorities must receive training in original classification as provided in this order and its implementing directives.

(e) Exceptional cases. When an employee, contractor, licensee, certificate holder, or grantee of an agency that does not have original classification authority originates information believed by that person to require classification, the information shall be protected in a manner consistent with this order and its implementing directives. The information shall be transmitted promptly as provided under this order or its implementing directives to the agency that has appropriate subject matter interest and classification authority with respect to this information. That agency shall decide within 30 days whether to classify this information. If it is not clear which agency has classification responsibility for this information, it shall be sent to the Director of the Information Security Oversight Office. The Director shall determine the agency having primary subject matter interest and forward the information, with appropriate recommendations, to that agency for a classification determination.

Sec. 1.5. *Classification Categories.*

Information may not be considered for classification unless it concerns:

(a) military plans, weapons systems, or operations;

(b) foreign government information;

(c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;

(d) foreign relations or foreign activities of the United States, including confidential sources;

(e) scientific, technological, or economic matters relating to the national security;

(f) United States Government programs for safeguarding nuclear materials or facilities; or

(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

Sec. 1.6. *Duration of Classification.* (a) At the time of original classification, the original classification authority shall attempt to establish a specific date

or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below.

(b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below.

(c) An original classification authority may extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to:

(1) reveal an intelligence source, method, or activity, or a cryptologic system or activity;
(2) reveal information that would assist in the development or use of weapons of mass destruction;
(3) reveal information that would impair the development or use of technology within a United States weapons system;
(4) reveal United States military plans, or national security emergency preparedness plans;
(5) reveal foreign government information;
(6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above;
(7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or
(8) violate a statute, treaty, or international agreement.

(e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order.

Sec. 1.7. *Identification and Markings.* (a) At the time of original classification, the following shall appear on the face of each classified document, or shall be applied to other classified media in an appropriate manner:

(1) one of the three classification levels defined in section 1.3 of this order;
(2) the identity, by name or personal identifier and position, of the original classification authority;
(3) the agency and office of origin, if not otherwise evident;
(4) declassification instructions, which shall indicate one of the following:
(A) the date or event for declassification, as prescribed in section 1.6(a) or section 1.6(c); or
(B) the date that is 10 years from the date of original classification, as prescribed in section 1.6(b); or
(C) the exemption category from declassification, as prescribed in section 1.6(d); and
(5) a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order.

(b) Specific information contained in paragraph (a), above, may be excluded if it would reveal additional classified information.

(c) Each classified document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, which portions are exempt from declassification under section 1.6(d) of this order, and which portions are unclassified. In accordance with standards prescribed in directives issued under this order, the Director of the Information Security Oversight Office may grant waivers of this requirement for specified classes of documents or information. The Director shall revoke any waiver upon a finding of abuse.

(d) Markings implementing the provisions of this order, including abbreviations and requirements to safeguard classified working papers, shall conform to the standards prescribed in implementing directives issued pursuant to this order.

(e) Foreign government information shall retain its original classification markings or shall be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.

(f) Information assigned a level of classification under this or predecessor orders shall be considered as classified at that level of classification despite the omission of other required markings. Whenever such information is used in the derivative classification process or is reviewed for possible declassification, holders of such information shall coordinate with an appropriate classification authority for the application of omitted markings.

(g) The classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document.

Sec. 1.8. *Classification Prohibitions and Limitations.* (a) In no case shall information be classified in order to:

(1) conceal violations of law, inefficiency, or administrative error;
(2) prevent embarrassment to a person, organization, or agency;
(3) restrain competition; or
(4) prevent or delay the release of information that does not require protection in the interest of national security.

(b) Basic scientific research information not clearly related to the national security may not be classified.

(c) Information may not be reclassified after it has been declassified and released to the public under proper authority.

(d) Information that has not previously been disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), or the mandatory review provisions of section 3.6 of this order only if such classification meets the requirements of this order and is accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official designated under section 5.6 of this order. This provision does not apply to classified information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code.

(e) Compilations of items of information which are individually unclassified may be classified if the compiled information reveals an additional association or relationship that:

(1) meets the standards for classification under this order; and
(2) is not otherwise revealed in the individual items of information.

As used in this order, "compilation" means an aggregation of pre-existing unclassified items of information.

Sec. 1.9. *Classification Challenges.* (a) Authorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information in accordance with agency procedures established under paragraph (b), below.

(b) In accordance with implementing directives issued pursuant to this order, an agency head or senior agency official shall establish procedures under which authorized holders of information are encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified. These procedures shall assure that:

(1) individuals are not subject to retribution for bringing such actions;

(2) an opportunity is provided for review by an impartial official or panel; and

(3) individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established by section 5.4 of this order.

PART 2—DERIVATIVE CLASSIFICATION

Sec. 2.1. *Definitions.* For purposes of this order:

(a) "Derivative classification" means the incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

(b) "Classification guidance" means any instruction or source that prescribes the classification of specific information.

(c) "Classification guide" means a documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

(d) "Source document" means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

(e) "Multiple sources" means two or more source documents, classification guides, or a combination of both.

Sec. 2.2. *Use of Derivative Classification.* (a) Persons who only reproduce, extract, or summarize classified information, or who only apply classification markings derived from source material or as directed by a classification guide, need not possess original classification authority.

(b) Persons who apply derivative classification markings shall:

(1) observe and respect original classification decisions; and

(2) carry forward to any newly created documents the pertinent classification markings. For information derivatively classified based on multiple sources, the derivative classifier shall carry forward:

(A) the date or event for declassification that corresponds to the longest period of classification among the sources; and

(B) a listing of these sources on or attached to the official file or record copy.

Sec. 2.3. *Classification Guides.* (a) Agencies with original classification authority shall prepare classification guides to facilitate the proper and uniform derivative classification of information. These guides shall conform to standards contained in directives issued under this order.

(b) Each guide shall be approved personally and in writing by an official who:

(1) has program or supervisory responsibility over the information or is the senior agency official; and

(2) is authorized to classify information originally at the highest level of classification prescribed in the guide.

(c) Agencies shall establish procedures to assure that classification guides are reviewed and updated as provided in directives issued under this order.

PART 3—DECLASSIFICATION AND DOWNGRADING

Sec. 3.1. *Definitions.* For purposes of this order:

(a) "Declassification" means the authorized change in the status of information from classified information to unclassified information.

(b) "Automatic declassification" means the declassification of information based solely upon:

(1) the occurrence of a specific date or event as determined by the original classification authority; or

(2) the expiration of a maximum time frame for duration of classification established under this order.

(c) "Declassification authority" means:

(1) the official who authorized the original classification, if that official is still serving in the same position;

(2) the originator's current successor in function;

(3) a supervisory official of either; or

(4) officials delegated declassification authority in writing by the agency head or the senior agency official.

(d) "Mandatory declassification review" means the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.6 of this order.

(e) "Systematic declassification review" means the review for declassification of classified information contained in records that have been determined by the Archivist of the United States ("Archivist") to have permanent historical value in accordance with chapter 33 of title 44, United States Code.

(f) "Declassification guide" means written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified.

(g) "Downgrading" means a determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level.

(h) "File series" means documentary material, regardless of its physical form or characteristics, that is arranged in accordance with a filing system or maintained as a unit because it pertains to the same function or activity.

Sec. 3.2. *Authority for Declassification.* (a) Information shall be declassified as soon as it no longer meets the standards for classification under this order.

(b) It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure. This provision does not:

(1) amplify or modify the substantive criteria or procedures for classification; or

(2) create any substantive or procedural rights subject to judicial review.

(c) If the Director of the Information Security Oversight Office determines that information is classified in violation of this order, the Director may require the information to be declassified by the agency that originated

the classification. Any such decision by the Director may be appealed to the President through the Assistant to the President for National Security Affairs. The information shall remain classified pending a prompt decision on the appeal.

(d) The provisions of this section shall also apply to agencies that, under the terms of this order, do not have original classification authority, but had such authority under predecessor orders.

Sec. 3.3. *Transferred Information.* (a) In the case of classified information transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving agency shall be deemed to be the originating agency for purposes of this order.

(b) In the case of classified information that is not officially transferred as described in paragraph (a), above, but that originated in an agency that has ceased to exist and for which there is no successor agency, each agency in possession of such information shall be deemed to be the originating agency for purposes of this order. Such information may be declassified or downgraded by the agency in possession after consultation with any other agency that has an interest in the subject matter of the information.

(c) Classified information accessioned into the National Archives and Records Administration ("National Archives") as of the effective date of this order shall be declassified or downgraded by the Archivist in accordance with this order, the directives issued pursuant to this order, agency declassification guides, and any existing procedural agreement between the Archivist and the relevant agency head.

(d) The originating agency shall take all reasonable steps to declassify classified information contained in records determined to have permanent historical value before they are accessioned into the National Archives. However, the Archivist may require that records containing classified information be accessioned into the National Archives when necessary to comply with the provisions of the Federal Records Act. This provision does not apply to information being transferred to the Archivist pursuant to section 2203 of title 44, United States Code, or information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that goes out of existence.

(e) To the extent practicable, agencies shall adopt a system of records management that will facilitate the public release of documents at the time such documents are declassified pursuant to the provisions for automatic declassification in sections 1.6 and 3.4 of this order.

Sec. 3.4. *Automatic Declassification.* (a) Subject to paragraph (b), below, within 5 years from the date of this order, all classified information contained in records that (1) are more than 25 years old, and (2) have been determined to have permanent historical value under title 44, United States Code, shall be automatically declassified whether or not the records have been reviewed. Subsequently, all classified information in such records shall be automatically declassified no longer than 25 years from the date of its original classification, except as provided in paragraph (b), below.

(b) An agency head may exempt from automatic declassification under paragraph (a), above, specific information, the release of which should be expected to:

(1) reveal the identity of a confidential human source, or reveal information about the application of an intelligence source or method, or reveal the identity of a human intelligence source when the unauthorized disclosure of that source would clearly and demonstrably damage the national security interests of the United States;
(2) reveal information that would assist in the development or use of weapons of mass destruction;
(3) reveal information that would impair U.S. cryptologic systems or activities;
(4) reveal information that would impair the application of state of the art technology within a U.S. weapon system;

(5) reveal actual U.S. military war plans that remain in effect;
(6) reveal information that would seriously and demonstrably impair relations between the United States and a foreign government, or seriously and demonstrably undermine ongoing diplomatic activities of the United States;
(7) reveal information that would clearly and demonstrably impair the current ability of United States Government officials to protect the President, Vice President, and other officials for whom protection services, in the interest of national security, are authorized;
(8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans; or
(9) violate a statute, treaty, or international agreement.

(c) No later than the effective date of this order, an agency head shall notify the President through the Assistant to the President for National Security Affairs of any specific file series of records for which a review or assessment has determined that the information within those file series almost invariably falls within one or more of the exemption categories listed in paragraph (b), above, and which the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the file series;
(2) an explanation of why the information within the file series is almost invariably exempt from automatic declassification and why the information must remain classified for a longer period of time; and
(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information.

The President may direct the agency head not to exempt the file series or to declassify the information within that series at an earlier date than recommended.

(d) At least 180 days before information is automatically declassified under this section, an agency head or senior agency official shall notify the Director of the Information Security Oversight Office, serving as Executive Secretary of the Interagency Security Classification Appeals Panel, of any specific information beyond that included in a notification to the President under paragraph (c), above, that the agency proposes to exempt from automatic declassification. The notification shall include:

(1) a description of the information;
(2) an explanation of why the information is exempt from automatic declassification and must remain classified for a longer period of time; and
(3) except for the identity of a confidential human source or a human intelligence source, as provided in paragraph (b), above, a specific date or event for declassification of the information. The Panel may direct the agency not to exempt the information or to declassify it at an earlier date than recommended. The agency head may appeal such a decision to the President through the Assistant to the President for National Security Affairs. The information will remain classified while such an appeal is pending.

(e) No later than the effective date of this order, the agency head or senior agency official shall provide the Director of the Information Security Oversight Office with a plan for compliance with the requirements of this section, including the establishment of interim target dates. Each such plan shall include the requirement that the agency declassify at least 15 percent of the records affected by this section no later than 1 year from the effective date of this order, and similar commitments for subsequent years until the effective date for automatic declassification.

(f) Information exempted from automatic declassification under this section shall remain subject to the mandatory and systematic declassification review provisions of this order.

(g) The Secretary of State shall determine when the United States should commence negotiations with the appropriate officials of a foreign government or international organization of governments to modify any treaty or international agreement that requires the classification of information contained in records affected by this section for a period longer than 25 years from the date of its creation, unless the treaty or international agreement pertains to information that may otherwise remain classified beyond 25 years under this section.

Sec. 3.5. *Systematic Declassification Review.* (a) Each agency that has originated classified information under this order or its predecessors shall establish and conduct a program for systematic declassification review. This program shall apply to historically valuable records exempted from automatic declassification under section 3.4 of this order. Agencies shall prioritize the systematic review of records based upon:

(1) recommendations of the Information Security Policy Advisory Council, established in section 5.5 of this order, on specific subject areas for systematic review concentration; or

(2) the degree of researcher interest and the likelihood of declassification upon review.

(b) The Archivist shall conduct a systematic declassification review program for classified information: (1) accessioned into the National Archives as of the effective date of this order; (2) information transferred to the Archivist pursuant to section 2203 of title 44, United States Code; and (3) information for which the National Archives and Records Administration serves as the custodian of the records of an agency or organization that has gone out of existence. This program shall apply to pertinent records no later than 25 years from the date of their creation. The Archivist shall establish priorities for the systematic review of these records based upon the recommendations of the Information Security Policy Advisory Council; or the degree of researcher interest and the likelihood of declassification upon review. These records shall be reviewed in accordance with the standards of this order, its implementing directives, and declassification guides provided to the Archivist by each agency that originated the records. The Director of the Information Security Oversight Office shall assure that agencies provide the Archivist with adequate and current declassification guides.

(c) After consultation with affected agencies, the Secretary of Defense may establish special procedures for systematic review for declassification of classified cryptologic information, and the Director of Central Intelligence may establish special procedures for systematic review for declassification of classified information pertaining to intelligence activities (including special activities), or intelligence sources or methods.

Sec. 3.6. *Mandatory Declassification Review.* (a) Except as provided in paragraph (b), below, all information classified under this order or predecessor orders shall be subject to a review for declassification by the originating agency if:

(1) the request for a review describes the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort;

(2) the information is not exempted from search and review under the Central Intelligence Agency Information Act; and

(3) the information has not been reviewed for declassification within the past 2 years. If the agency has reviewed the information within the past 2 years, or the information is the subject of pending litigation, the agency shall inform the requester of this fact and of the requester's appeal rights.

(b) Information originated by:

(1) the incumbent President;

(2) the incumbent President's White House Staff;

(3) committees, commissions, or boards appointed by the incumbent President; or

(4) other entities within the Executive Office of the President that solely advise and assist the incumbent President is exempted from the provisions of paragraph (a), above. However, the Archivist shall have the authority to review, downgrade, and declassify information of former Presidents under the control of the Archivist pursuant to sections 2107, 2111, 2111 note, or 2203 of title 44, United States Code. Review procedures developed by the Archivist shall provide for consultation with agencies having primary subject matter interest and shall be consistent with the provisions of applicable laws or lawful agreements that pertain to the respective Presidential papers or records. Agencies with primary subject matter interest shall be notified promptly of the Archivist's decision. Any final decision by the Archivist may be appealed by the requester or an agency to the Interagency Security Classification Appeals Panel. The information shall remain classified pending a prompt decision on the appeal.

(c) Agencies conducting a mandatory review for declassification shall declassify information that no longer meets the standards for classification under this order. They shall release this information unless withholding is otherwise authorized and warranted under applicable law.

(d) In accordance with directives issued pursuant to this order, agency heads shall develop procedures to process requests for the mandatory review of classified information. These procedures shall apply to information classified under this or predecessor orders. They also shall provide a means for administratively appealing a denial of a mandatory review request, and for notifying the requester of the right to appeal a final agency decision to the Interagency Security Classification Appeals Panel.

(e) After consultation with affected agencies, the Secretary of Defense shall develop special procedures for the review of cryptologic information, the Director of Central Intelligence shall develop special procedures for the review of information pertaining to intelligence activities (including special activities), or intelligence sources or methods, and the Archivist shall develop special procedures for the review of information accessioned into the National Archives.

Sec. 3.7. *Processing Requests and Reviews.* In response to a request for information under the Freedom of Information Act, the Privacy Act of 1974, or the mandatory review provisions of this order, or pursuant to the automatic declassification or systematic review provisions of this order:

(a) An agency may refuse to confirm or deny the existence or nonexistence of requested information whenever the fact of its existence or nonexistence is itself classified under this order.

(b) When an agency receives any request for documents in its custody that contain information that was originally classified by another agency, or comes across such documents inthe process of the automatic declassification or systematic review provisions of this order, it shall refer copies of any request and the pertinent documents to the originating agency for processing, and may, after consultation with the originating agency, inform any requester of the referral unless such association is itself classified under this order. In cases in which the originating agency determines in writing that a response under paragraph (a), above, is required, the referring agency shall respond to the requester in accordance with that paragraph.

Sec. 3.8. *Declassification Database.* (a) The Archivist in conjunction with the Director of the Information Security Oversight Office and those agencies that originate classified information, shall establish a Governmentwide database of information that has been declassified. The Archivist shall also explore other possible uses of technology to facilitate the declassification process.

(b) Agency heads shall fully cooperate with the Archivist in these efforts.

(c) Except as otherwise authorized and warranted by law, all declassified information contained within the database established under paragraph (a), above, shall be available to the public.

PART 4—SAFEGUARDING

Sec. 4.1. *Definitions.* For purposes of this order: (a) "Safeguarding" means measures and controls that are prescribed to protect classified information.

(b) "Access" means the ability or opportunity to gain knowledge of classified information.

(c) "Need-to-know" means a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

(d) "Automated information system" means an assembly of computer hardware, software, or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information.

(e) "Integrity" means the state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed.

(f) "Network" means a system of two or more computers that can exchange data or information.

(g) "Telecommunications" means the preparation, transmission, or communication of information by electronic means.

(h) "Special access program" means a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Sec. 4.2. *General Restrictions on Access.* (a) A person may have access to classified information provided that:

(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;

(2) the person has signed an approved nondisclosure agreement; and

(3) the person has a need-to-know the information.

(b) Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

(c) Classified information may not be removed from official premises without proper authorization.

(d) Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

(e) Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process, or store classified information have controls that:

(1) prevent access by unauthorized persons; and

(2) ensure the integrity of the information.

(f) Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

(g) Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a need-to-know who have not otherwise been cleared for access to classified information or executed an approved nondisclosure agreement.

(h) Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

Sec. 4.3. *Distribution Controls.* (a) Each agency shall establish controls over the distribution of classified information to assure that it is distributed only to organizations or individuals eligible for access who also have a need-to-know the information.

(b) Each agency shall update, at least annually, the automatic, routine, or recurring distribution of classified information that they distribute. Recipients shall cooperate fully with distributors who are updating distribution lists and shall notify distributors whenever a relevant change in status occurs.

Sec. 4.4. *Special Access Programs.* (a) Establishment of special access programs. Unless otherwise authorized by the President, only the Secretaries of State, Defense and Energy, and the Director of Central Intelligence, or the principal deputy of each, may create a special access program. For special access programs pertaining to intelligence activities (including special activities, but not including military operational, strategic and tactical programs), or intelligence sources or methods, this function will be exercised by the Director of Central Intelligence. These officials shall keep the number of these programs at an absolute minimum, and shall establish them only upon a specific finding that:

(1) the vulnerability of, or threat to, specific information is exceptional; and

(2) the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure; or

(3) the program is required by statute.

(b) *Requirements and Limitations.* (1) Special access programs shall be limited to programs in which the number of persons who will have access ordinarily will be reasonably small and commensurate with the objective of providing enhanced protection for the information involved.

(2) Each agency head shall establish and maintain a system of accounting for special access programs consistent with directives issued pursuant to this order.

(3) Special access programs shall be subject to the oversight program established under section 5.6(c) of this order. In addition, the Director of the Information Security Oversight Office shall be afforded access to these programs, in accordance with the security requirements of each program, in order to perform the functions assigned to the Information Security Oversight Office under this order. An agency head may limit access to a special access program to the Director and no more than one other employee of the Information Security Oversight Office; or, for special access programs that are extraordinarily sensitive and vulnerable, to the Director only.

(4) The agency head or principal deputy shall review annually each special access program to determine whether it continues to meet the requirements of this order.

(5) Upon request, an agency shall brief the Assistant to the President for National Security Affairs, or his or her designee, on any or all of the agency's special access programs.

(c) Within 180 days after the effective date of this order, each agency head or principal deputy shall review all existing special access programs under the agency's jurisdiction. These officials shall terminate any special access programs that do not clearly meet the provisions of this order. Each existing special access program that an agency head or principal deputy validates shall be treated as if it were established on the effective date of this order.

(d) Nothing in this order shall supersede any requirement made by or under 10 U.S.C. 119.

Sec. 4.5. *Access by Historical Researchers and Former Presidential Appointees.* (a) The requirement in section 4.2(a)(3) of this order that access to classified information may be granted only to individuals who have a need-to-know the information may be waived for persons who:

(1) are engaged in historical research projects; or

(2) previously have occupied policy-making positions to which they were appointed by the President.

(b) Waivers under this section may be granted only if the agency head or senior agency official of the originating agency:

(1) determines in writing that access is consistent with the interest of national security;

(2) takes appropriate steps to protect classified information from unauthorized disclosure or compromise, and ensures that the information is safeguarded in a manner consistent with this order; and

(3) limits the access granted to former Presidential appointees to items that the person originated, reviewed, signed, or received while serving as a Presidential appointee.

PART 5—IMPLEMENTATION AND REVIEW

Sec. 5.1. *Definitions.* For purposes of this order: (a) "Self-inspection" means the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under this order and its implementing directives.

(b) "Violation" means:

(1) any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information;

(2) any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of this order or its implementing directives; or

(3) any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of this order.

(c) "Infraction" means any knowing, willful, or negligent action contrary to the requirements of this order or its implementing directives that does not comprise a "violation," as defined above.

Sec. 5.2. *Program Direction.* (a) The Director of the Office of Management and Budget, in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board, shall issue such directives as are necessary to implement this order. These directives shall be binding upon the agencies. Directives issued by the Director of the Office of Management and Budget shall establish standards for:

(1) classification and marking principles;

(2) agency security education and training programs;

(3) agency self-inspection programs; and

(4) classification and declassification guides.

(b) The Director of the Office of Management and Budget shall delegate the implementation and monitorship functions of this program to the Director of the Information Security Oversight Office.

(c) The Security Policy Board, established by a Presidential Decision Directive, shall make a recommendation to the President through the Assistant to the President for National Security Affairs with respect to the issuance of a Presidential directive on safeguarding classified information. The Presidential directive shall pertain to the handling, storage, distribution, transmittal, and destruction of and accounting for classified information.

Sec. 5.3. *Information Security Oversight Office.* (a) There is established within the Office of Management and Budget an Information Security Oversight Office. The Director of the Office of Management and Budget shall appoint the Director of the Information Security Oversight Office, subject to the approval of the President.

(b) Under the direction of the Director of the Office of Management and Budget acting in consultation with the Assistant to the President for National Security Affairs, the Director of the Information Security Oversight Office shall:

(1) develop directives for the implementation of this order;

(2) oversee agency actions to ensure compliance with this order and its implementing directives;

(3) review and approve agency implementing regulations and agency guides for systematic declassification review prior to their issuance by the agency;

(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports, information, and other cooperation that may be necessary to fulfill its responsibilities. If granting access to specific categories of classified information would pose an exceptional national security risk, the affected agency head or the senior agency official shall submit a written justification recommending the denial of access to the Director of the Office of Management and Budget within 60 days of the request for access. Access shall be denied pending a prompt decision by the Director of the Office of Management and Budget, who shall consult on this decision with the Assistant to the President for National Security Affairs;

(5) review requests for original classification authority from agencies or officials not granted original classification authority and, if deemed appropriate, recommend Presidential approval through the Director of the Office of Management and Budget;

(6) consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the program established under this order;

(7) have the authority to prescribe, after consultation with affected agencies, standardization of forms or procedures that will promote the implementation of the program established under this order;

(8) report at least annually to the President on the implementation of this order; and

(9) convene and chair interagency meetings to discuss matters pertaining to the program established by this order.

Sec. 5.4. *Interagency Security Classification Appeals Panel.*

(a) Establishment and Administration.

(1) There is established an Interagency Security Classification Appeals Panel ("Panel"). The Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the Assistant to the President for National Security Affairs shall each appoint a senior level representative to serve as a member of the Panel. The President shall select the Chair of the Panel from among the Panel members.

(2) A vacancy on the Panel shall be filled as quickly as possible as provided in paragraph (1), above.

(3) The Director of the Information Security Oversight Office shall serve as the Executive Secretary. The staff of the Information Security Oversight Office shall provide program and administrative support for the Panel.

(4) The members and staff of the Panel shall be required to meet eligibility for access standards in order to fulfill the Panel's functions.

(5) The Panel shall meet at the call of the Chair. The Chair shall schedule meetings as may be necessary for the Panel to fulfill its functions in a timely manner.

(6) The Information Security Oversight Office shall include in its reports to the President a summary of the Panel's activities.

(b) *Functions.* The Panel shall:

(1) decide on appeals by persons who have filed classification challenges under section 1.9 of this order;

(2) approve, deny, or amend agency exemptions from automatic declassification as provided in section 3.4 of this order; and

(3) decide on appeals by persons or entities who have filed requests for mandatory declassification review under section 3.6 of this order.

(c) *Rules and Procedures.* The Panel shall issue bylaws, which shall be published in the Federal Register no later than 120 days from the effective date of this order. The bylaws shall establish the rules and procedures that the Panel will follow in accepting, considering, and issuing decisions on appeals. The rules and procedures of the Panel shall provide that the Panel will consider appeals only on actions in which: (1) the appellant has exhausted his or her administrative remedies within the responsible agency; (2) there is no current action pending on the issue within the federal courts; and (3) the information has not been the subject of review by the federal courts or the Panel within the past 2 years.

(d) Agency heads will cooperate fully with the Panel so that it can fulfill its functions in a timely and fully informed manner. An agency head may appeal a decision of the Panel to the President through the Assistant to the President for National Security Affairs. The Panel will report to the President through the Assistant to the President for National Security Affairs any instance in which it believes that an agency head is not cooperating fully with the Panel.

(e) The Appeals Panel is established for the sole purpose of advising and assisting the President in the discharge of his constitutional and discretionary authority to protect the national security of the United States. Panel decisions are committed to the discretion of the Panel, unless reversed by the President.

Sec. 5.5. *Information Security Policy Advisory Council.*

(a) *Establishment.* There is established an Information Security Policy Advisory Council ("Council"). The Council shall be composed of seven members appointed by the President for staggered terms not to exceed 4 years, from among persons whohave demonstrated interest and expertise in an area related to the subject matter of this order and are not otherwise employees of the Federal Government. The President shall appoint the Council Chair from among the members. The Council shall comply with the Federal Advisory Committee Act, as amended, 5 U.S.C. App. 2.

(b) *Functions.* The Council shall:

(1) advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, or such other executive branch officials as it deems appropriate, on policies established under this order or its implementing directives, including recommended changes to those policies;

(2) provide recommendations to agency heads for specific subject areas for systematic declassification review; and

(3) serve as a forum to discuss policy issues in dispute.

(c) *Meetings.* The Council shall meet at least twice each calendar year, and as determined by the Assistant to the President for National Security Affairs or the Director of the Office of Management and Budget.

(d) *Administration.*

(1) Each Council member may be compensated at a rate of pay not to exceed the daily equivalent of the annual rate of basic pay in effect for grade GS-18 of the general schedule under section 5376 of title 5, United States Code, for each day during which that member is engaged in the actual performance of the duties of the Council.

(2) While away from their homes or regular place of business in the actual performance of the duties of the Council, members may be allowed travel expenses, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5703(b)).

(3) To the extent permitted by law and subject to the availability of funds, the Information Security Oversight Office shall provide the Council with administrative services, facilities, staff, and other support services necessary for the performance of its functions.

(4) Notwithstanding any other Executive order, the functions of the President under the Federal Advisory Committee Act, as amended, that are applicable to the Council, except that of reporting to the Congress, shall be performed by the Director of the Information Security Oversight Office in accordance with the guidelines and procedures established by the General Services Administration.

Sec. 5.6. *General Responsibilities.* Heads of agencies that originate or handle classified information shall:

(a) demonstrate personal commitment and commit senior management to the successful implementation of the program established under this order;

(b) commit necessary resources to the effective implementation of the program established under this order; and

(c) designate a senior agency official to direct and administer the program, whose responsibilities shall include:

(1) overseeing the agency's program established under this order, provided, an agency head may designate a separate official to oversee special access programs authorized under this order. This official shall provide a full accounting of the agency's special access programs at least annually;

(2) promulgating implementing regulations, which shall be published in the **Federal Register** to the extent that they affect members of the public;

(3) establishing and maintaining security education and training programs;

(4) establishing and maintaining an ongoing self-inspection program, which shall include the periodic review and assessment of the agency's classified product;

(5) establishing procedures to prevent unnecessary access to classified information, including procedures that: (i) require that a need for access to classified information is established before initiating administrative clearance procedures; and (ii) ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs;

(6) developing special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas;

(7) assuring that the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element or item to be evaluated in the rating of: (i) original classification authorities; (ii) security managers or security specialists; and (iii) all other personnel whose duties significantly involve the creation or handling of classified information;

(8) accounting for the costs associated with the implementation of this order, which shall be reported to the Director of the Information Security Oversight Office for publication; and

(9) assigning in a prompt manner agency personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of this order that pertains to classified information that originated in a component of the agency that no longer exists and for which there is no clear successor in function.

Sec. 5.7. *Sanctions.* (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives may have occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.

(b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, willfully, or negligently:

(1) disclose to unauthorized persons information properly classified under this order or predecessor orders;

(2) classify or continue the classification of information in violation of this order or any implementing directive;

(3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b), above, occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3), above, occurs.

PART 6—GENERAL PROVISIONS

Sec. 6.1. *General Provisions.* (a) Nothing in this order shall supersede any requirement made by or under the Atomic Energy Act of 1954, as amended, or the National Security Act of 1947, as amended. "Restricted Data" and "Formerly Restricted Data" shall be handled, protected, classified, downgraded, and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and regulations issued under that Act.

(b) The Attorney General, upon request by the head of an agency or the Director of the Information Security Oversight Office, shall render an interpretation of this order with respect to any question arising in the course of its administration.

(c) Nothing in this order limits the protection afforded any information by other provisions of law, including the exemptions to the Freedom of Information Act, the Privacy Act, and the National Security Act of 1947, as amended. This order is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law by a party against the United States, its agencies, itsofficers, or its employees. The foregoing is in addition to the specific provisos set forth in sections 1.2(b), 3.2(b) and 5.4(e) of this order.

(d) Executive Order No. 12356 of April 6, 1982, is revoked as of the effective date of this order.

Sec. 6.2. *Effective Date.* This order shall become effective 180 days from the date of this order.

William J. Clinton

THE WHITE HOUSE,
April 17, 1995.

[FR Doc. 95-9941
Filed 4-18-95; 2:04 pm]
Billing code 3195-01-P

This Page Intentionally Left Blank

NTISS Policy

This Page Intentionally Left Blank

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

NATIONAL POLICY

ON

PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION

IN FEDERAL GOVERNMENT TELECOMMUNICATIONS

AND AUTIOMATED INFORMATION SYSTEMS

CHAIRMAN

FOREWORD

NSDD-145, "National Policy on Telecommunications and Automated Information Systems Security," signed by the President on 17 September 1984, in part provides policy and direction for systems protection and safeguards for telecommunications and automated information systems that process or communicate sensitive but unclassified information. The NSDD-145 Systems Security Steering Group has established that sensitive, but unclassified information that could adversely affect national security or other Federal Government interests shall have system protection and safeguards; however, the determination of what is sensitive, but unclassified information is a responsibility of Agency heads. Executive order 12356 prescribes requirements for classifying, declassifying, and safeguarding national security information.

This policy and the principles and procedures contained in Office of Management and Budget (OMB) Circulars Nos. A-123 and A-130, "Management of Federal Information Resources," are complementary.

9 I X_-
John M. Poindexter

NATIONAL POLICY ON PROTECTION OF SENSITIVE, BUT UNCLASSIFIED INFORMATION IN FEDERAL GOVERNMENT TELECOMMUNICATIONS AND AUTOMATED INFORMATION SYSTEMS

SECTION I - POLICY

Federal Departments and Agencies shall ensure that telecommunications and automated information systems handling sensitive, but unclassified information will protect such information to the level of risk and the magnitude of loss or harm that could result from disclosure, loss, misuse, alteration, or destruction.

SECTION 11 - DEFINITION

Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and Law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens.

SECTION III - APPLICABILITY

This policy applies to all Federal Executive Branch Departments and Agencies, and entities, including their contractors, which electronically transfer, store, process, or communicate sensitive, but unclassified information.

SECTION IV - RESPONSIBILITIES

This policy assigns to the heads of Federal Government Departments and Agencies the responsibility to determine what information is sensitive, but unclassified and to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems. The Director of Central Intelligence shall, in addition, be responsible for identifying sensitive, but unclassified information bearing on intelligence sources and methods and for establishing the system security handling procedures and the protection required for such information.

Federal Government Department and Agency heads shall:

a. Determine which of their department's or agency's information is sensitive but unclassified and may warrant protection as sensitive during communications or processing via telecommunications or automated information systems. This determination should be based on the department's or agency's responsibilities, policies, and experience, and those requirements imposed by Federal statutes, as well as National Manager guidance on areas that potential adversaries have targeted;

b. Identify the systems which electronically process, store, transfer, or communicate sensitive, unclassified information requiring protection;

c. Determine, in coordination with the National Manager, as appropriate the threat to and the vulnerability of those identified systems and;

d. Develop, fund and implement telecommunications and automated information security to the extent consistent with their mission responsibilities and in coordination with the National Manager, as appropriate, to satisfy their security or protection requirements.

e. Ensure implementation of telecommunications and automated information systems security consistent with the procedures and safeguards set forth in OMB Circular A-123 and A-130.

The National Manager shall, when requested, assist, Federal Government Departments and Agencies to assess the threat to and vulnerability of targeted systems, to identify and document their telecommunications and automated information systems protection needs, and to develop the necessary security architectures.

Economic Espionage Act of 1996

Title I - Protection of Trade Secrets
Sec. 101. Protection of Trade Secrets

(a) In General.-Title 18, United States Code, is amended by inserting after chapter 89 the following:

Sec.

1831. Economic espionage.

1832. Theft of trade secrets.

1833. Exceptions to prohibitions.

1834. Criminal forfeiture.

1835. Orders to preserve confidentiality.

1836. Civil proceedings to enjoin violations.

1837. Conduct outside the United States.

1838. Construction with other laws.

1839. Definitions.

Chapter 90-

Protection of Trade Secrets

Section 1831 Economic espionage

(a) In General - Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret,
(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization,
(4) attempts to commit any offense described in any of paragraphs (1) through (3), or
(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

(b) Organizations - Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

Section 1832. Theft of trade secrets.

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly -

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
(4) attempts to commit any offense described in paragraphs (1) through (3); or
(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

Section 1833. Exceptions to prohibitions.

This chapter does not prohibit -

(1) any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State; or

(2) the reporting of a suspected violation of law to any governmental entity of the United States, a State, or a political subdivision of a State, if such entity has lawful authority with respect to that violation.

Section 1834. Criminal forfeiture.

(a) The court, in imposing sentence on a person for a violation of this chapter, shall order, in addition to any other sentence imposed, that the person forfeit to the United States -

(1) any property constituting or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and

(2) any of the person's or organization's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking into consideration the nature, scope, and proportionality of the use of the property in the offense.

(b) Property subject to forfeiture under this section, any seizure and disposition thereof, and any administrative or judicial proceeding in relation thereto, shall be governed by section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S. C. 8 5 3), except for subsections (d) and 0) of such section, which shall not apply to forfeitures under this section.

Section 1835. Orders to preserve confidentiality

In any prosecution or other proceeding under this chapter, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

Section 1836. Civil proceedings to enjoin violations

(a) The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this section.

(b) The district courts of the United States shall have exclusive original jurisdiction of civil actions under this subsection.

Section 1837 Applicability to conduct outside the United States

This chapter also applies to conduct occurring outside the United States if

(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof-, or

(2) an act in furtherance of the offense was committed in the Untied States.

Section 1838 Construction with other laws

This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by Untied States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret, or to affect the otherwise lawful disclosure of information by any Government employees under section 552 of title 5 (commonly known as the Freedom of Information Act).

Section 1839 Definitions

As used in this chapter

(1) the term '*foreign instrumentality*' means any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government:

(2) the term '*foreign agent*' means any officer, employee, proxy, servant, delegate, or representative of a foreign government:

(3) the term '*trade secret*' means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically graphically, photographically, or in writing if

(a) the owner thereof has taken reasonable measures to keep such information secret; and

(b) the information derives independent economic value, actual or potential, from not being general known to, and not being readily ascertainable through proper means by the public, and

(4) the term 'owner', with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to or license in, the trade secret is reposed."

(b) Clerical Amendment. The table of chapters at the beginning part I of title 18, United States Code, is amended by inserting after the item relating to chapter 89 the following:

"90. Protection of trade secrets 1831"

(c) Reports. - Not later than 2 years and 4 years after the date of the enactment of this Congress of this Act, the Attorney General shall report to Congress on the amounts received and distributed from fines for offenses under this chapter deposited in the Crime Victims Fund established by section 1402 of the Victims of Crime Act of 1984 (42 U.S. C. 10601).

See. 102 Wire and Electronic Communications Interception and Interception of Oral Communications.

Section 2516(l)(c) of title 18, United States Code, is amended by inserting "chapter 90 (relating to protection of trade secrets)," after "chapter 37 (relating to espionage),"

Passed by Congress: October 2, 1996
Signed by the President: October 11, 1996

Defense Acquisition Circular 91-11

This Page Intentionally Left Blank

Defense Acquisition Circular 91-11

This Page last updated in or before DAC 09

SUBPART 227.71--RIGHTS IN TECHNICAL DATA

227.7100 Scope of subpart.

This subpart--

(a) Prescribes policies and procedures for the acquisition of technical data and the rights to use, modify, reproduce, release, perform, display, or disclose technical data. It implements requirements in the following laws and Executive Order:

(1) 10 U.S.C. 2302(4).
(2) 10 U.S.C. 2305 (subsection (d)(4)).
(3) 10 U.S.C. 2320.
(4) 10 U.S.C. 2321.
(5) 10 U.S.C. 2325.
(6) Pub. L. 103-355.
(7) Executive Order 12591 (Subsection 1(b)(6)).

(b) Does not apply to computer software or technical data that is computer software documentation (see Subpart 227.72).

227.7101 Definitions.

(a) As used in this subpart, unless otherwise specifically indicated, the terms "offeror" and "contractor" include an offeror's or contractor's subcontractors, suppliers, or potential subcontractors or suppliers at any tier.

(b) Other terms used in this subpart are defined in the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items.

227.7102 Commercial items, components, or processes.

Section 2320(b)(1) of Title 10 U.S.C. establishes a presumption that commercial items are developed at private expense whether or not a contractor submits a justification in response to a challenge notice. Therefore, do not challenge a contractor's assertion that a commercial item, component, or process was developed at private expense unless the Government can demonstrate that it contributed to development of the item, component or process. Follow the procedures in 227.7103-13 and the clause at 252.227-7037, Validation of Restrictive Markings on Technical Data, when information provided by the Department of Defense demonstrates that an item, component, or process was not developed exclusively at private expense. However, when a challenge is warranted, a contractor's or subcontractor's failure to respond to the challenge notice cannot be the sole basis for issuing a final decision denying the validity of an asserted restriction.

227.7102-1 Policy.

(a) DoD shall acquire only the technical data customarily provided to the public with a commercial item or process, except technical data that--
(1) Are form, fit, or function data;
(2) Are required for repair or maintenance of commercial items or processes, or for the proper installation, operating, or handling of a commercial item, either as a stand alone unit or as a part of a military system, when such data are not customarily provided to commercial users or the data provided to commercial users is not sufficient for military purposes; or
(3) Describe the modifications made at Government expense to a commercial item or process in order to meet the requirements of a Government solicitation.
(b) To encourage offerors and contractors to offer or use commercial products to satisfy military requirements, offerors and contractors shall not be required, except for the technical data described in paragraph (a) of this subsection, to--
(1) Furnish technical information related to commercial items or processes that is not customarily provided to the public; or
(2) Relinqu
ish to, or otherwise provide, the Government rights to use, modify, reproduce, release, perform, display, or disclose technical data pertaining to commercial items or processes except for a transfer of rights mutually agreed upon.

227.7102-2 Rights in technical data.

(a) The clause at 252.227-7015, Technical Data--Commercial Items, provides the Government specific license rights in technical data pertaining to commercial items or processes. DoD may use, modify, reproduce, release, perform, display, or disclose data only within the Government. The data may not be used to manufacture additional quantities of the commercial items and, except for emergency repair or overhaul, may not be released or disclosed to, or used by, third parties without the contractor's written permission. Those restrictions do not apply to the technical data described in 227.7102-1(a).
(b) If additional rights are needed, contracting activities must negotiate with the contractor to determine if there are acceptable terms for transferring such rights. The specific additional rights granted to the Government shall be enumerated in a license agreement made part of the contract.

227.7102-3 Contract clause.

(a) Except as provided in paragraph (b) of this subsection, use the clause at 252.227-7015, Technical Data--Commercial Items, in all solicitations and contracts when the contractor will be required to deliver technical data pertaining to commercial items, components, or processes. Do not require the contractor to include this clause in its subcontracts.
(b) Use the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, in lieu of the clause at 252.227-7015

if the Government will pay any portion of the development costs. Do not require the contractor to include this clause in its subcontracts for commercial items or commercial components.

(c) Use the clause at 252.227-7037, Validation of Restrictive Markings on Technical Data, in all solicitations and contracts for commercial items that include the clause at 252.227-7015 or the clause at 252.227-7013. Do not require the contractor to include this clause in its subcontracts for commercial items or commercial components.

227.7103 Noncommercial items or processes.

227.7103-1 Policy.

(a) DoD policy is to acquire only the technical data, and the rights in that data, necessary to satisfy agency needs.

(b) Solicitations and contracts shall--

(1) Specify the technical data to be delivered under a contract and delivery schedules for the data;

(2) Establish or reference procedures for determining the acceptability of technical data;

(3) Establish separate contract line items, to the extent practicable, for the technical data to be delivered under a contract and require offerors and contractors to price separately each deliverable data item; and

(4) Require offerors to identify, to the extent practicable, technical data to be furnished with restrictions on the Government's rights and require contractors to identify technical data to be delivered with such restrictions prior to delivery.

(c) Offerors shall not be required, either as a condition of being responsive to a solicitation or as a condition for award, to sell or otherwise relinquish to the Government any rights in technical data related to items, components or processes developed at private expese except for the data identified at 227.7103-5(a)(2) and (a)(4) through (9).

(d) Offerors and contractors shall not be prohibited or discouraged from furnishing or offering to furnish items, components, or processes developed at private expense solely because the Government's rights to use, modify, release, reproduce, perform, display, or disclose technical data pertaining to those items may be restricted.

(e) As provided in 10 U.S.C. 2305, solicitations for major systems development contracts shall not require offerors to submit proposals that would permit the Government to acquire competitively items identical to items developed at private expense unless a determination is made at a level above the contracting officer that--

(1) The offeror will not be able to satisfy program schedule or delivery requirements; or

(2) The offeror's proposal to meet mobilization requirements does not satisfy mobilization needs.

227.7103-2 Acquisition of technical data.

(a) Contracting officers shall work closely with data

managers and requirements personnel to assure that data requirements included in solicitations are consistent with the policy expressed in 227.7103-1.

(b)(1) Data managers or other requirements personnel are responsible for identifying the Government's minimum needs for technical data. Data needs must be established giving consideration to the contractor's economic interests in data pertaining to items, components, or processes that have been developed at private expense; the Government's costs to acquire, maintain, store, retrieve, and protect the data; reprocurement needs; repair, maintenance and overhaul philosophies; spare and repair part considerations; and whether procurement of the items, components, or processes can be accomplished on a form, fit, or function basis. When it is anticipated that the Government will obtain unlimited or government purpose rights in technical data that will be required for competitive spare or repair parts procurements, such data should be identified as deliverable data items. Reprocurement needs may not be a sufficient reason to acquire detailed manufacturing or process data when items or components can be acquired using performance specifications, form, fit and function data, or when there are a sufficient number of alternate sources which can reasonably be expected to provide such items on a performance specification or form, fit, or function basis.

(2) When reviewing offers received in response to a solicitation or other request for data, data managers must balance the original assessment of the Government's data needs with data prices contained in the offer.

(c) Contracting officers are responsible for ensuring that, wherever practicable, solicitations and contracts--

(1) Identify the type and quantity of the technical data to be delivered under the contract and the format and media in which the data will be delivered;

(2) Establish each deliverable data item as a separate contract line item (this requirement may be satisfied by listing each deliverable data item on an exhibit to the contract);

(3) Identify the prices established for each deliverable data item under a fixed-price type contract;

(4) Include delivery schedules and acceptance criteria for each deliverable data item; and

(5) Specifically identify the place of delivery for each deliverable item of technical data.

227.7103-3 Early identification of technical data to be furnished to the Government disclosure.

(a) 10 U.S.C. 2320 requires, to the maximum extent practicable, an identification prior to delivery of any technical data to be delivered to the Government with restrictions on use.

(b) Use the provision at 252.227-7017, Identification and Assertion of Use, Release, or Disclosure Restrictions, in all solicitations that include the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items. The provision requires offerors to identify any technical data for which restrictions, other than copyright, on use, release, or disclosure are asserted and to attach the identification and assertions to the offer.

(c) Subsequent to contract award, the clause at 252.227-7013 permits a contractor, under certain conditions, to make

additional assertions of use, release, or disclosure restrictions. The prescription for the use of that clause and its alternate is at 227.7103-6(a) and (b).

227.7103-4 License rights.

(a) Grant of license.

The Government obtains rights in technical data, including a copyright license, under an irrevocable license granted or obtained for the Government by the contractor. The contractor or licensor retains all rights in the data not granted to the Government. For technical data that pertain to items, components, or processes, the scope of the license is generally determined by the source of funds used to develop the item, component, or process. When the technical data do not pertain to items, components, or processes, the scope of the license is determined by the source of funds used to create the data.

(1) Technical data pertaining to items, components, or processes.

Contractors or licensors may, with some exceptions (see 227.7103-5(a)(2) and (a)(4) through (9)), restrict the Government's rights to use, modify, release, reproduce, perform, display or disclose technical data pertaining to items, components, or processes developed exclusively at private expense (limited rights). They may not restrict the Government's rights in items, components, or processes developed exclusively at Government expense (unlimited rights) without the Government's approval. When an item, component, or process is developed with mixed funding, the Government may use, modify, release, reproduce, perform, display or disclose the data pertaining to such items, components, or processes within the Government without restriction but may release or disclose the data outside the Government only for government purposes (government purpose rights).

(2) Technical data that do not pertain to items, components, or processes.

Technical data may be created during the performance of a contract for a conceptual design or similar effort that does not require the development, manufacture, construction, or production of items, components or processes. The Government generally obtains unlimited rights in such data when the data were created exclusively with Government funds, government purpose rights when the data were created with mixed funding, and limited rights when the data were created exclusively at private expense.

(b) Source of funds determination.

The determination of the source of development funds for technical data pertaining to items, components, or processes should be made at any practical sub-item or sub-component level or for any segregable portion of a process. Contractors may assert limited rights in a segregable sub-item, sub-component, or portion of a process which otherwise qualifies for limited rights under the clause at 252.227-7013 Rights in Technical Data--Noncommercial Items.

227.7103-5 Government rights.

The standard license rights that a licensor grants to the

Government are unlimited rights, government purpose rights, or limited rights. Those rights are defined in the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items. In unusual situations, the standard rights may not satisfy the Government's needs or the Government may be willing to accept lesser rights in data in return for other consideration. In those cases, a special license may be negotiated. However, the licensor is not obligated to provide the Government greater rights and the contracting officer is not required to accept lesser rights than the rights provided in the standard grant of license. The situations under which a particular grant of license applies are enumerated in paragraphs (a) through (d) of this subsection.

(a) Unlimited rights.

The Government obtains unlimited rights in technical data that are--

(1) Data pertaining to an item, component, or process which has been or will be developed exclusively with Government funds;

(2) Studies, analyses, test data, or similar data produced in the performance of a contract when the study, analysis, test, or similar work was specified as an element of performance;

(3) Created exclusively with Government funds in the performance of a contract that does not require the development, manufacture, construction, or production of items, components, or processes;

(4) Form, fit, and function data;

(5) Necessary for installation, operation, maintenance, or training purposes (other than detailed manufacturing or process data);

(6) Corrections or changes to technical data furnished to the contractor by the Government;

(7) Publicly available or have been released or disclosed by the contractor or subcontractor without restrictions on further use, release or disclosure other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the software to another party or the sale or transfer of some or all of a business entity or its assets to another party;

(8) Data in which the Government has obtained unlimited rights under another Government contract or as a result of negotiations; or

(9) Data furnished to the Government, under a Government contract or subcontract thereunder, with--

(i) Government purpose license rights or limited rights and the restrictive condition(s) has/have expired; or

(ii) Government purpose rights and the contractor's exclusive right to use such data for commercial purposes has expired.

(b) Government purpose rights.

(1) The Government obtains government purpose rights in technical data--

(i) That pertain to items, components, or processes developed with mixed funding except when the Government is entitled to unlimited rights as provided in paragraphs (a)(2) and (a)(4) through (9) of this subsection; or

(ii) Created with mixed funding in the performance of a contract that does not require the development, manufacture, construction, or production of items, components, or processes.

(2) The period during which government purpose rights are effective is negotiable. The clause at 252.227-7013

provides a nominal five-year period. Either party may request a different period. Changes to the government purpose rights period may be made at any time prior to delivery of the technical data without consideration from either party. Longer periods should be negotiated when a five-year period does not provide sufficient time to apply the data for commercial purposes or when necessary to recognize subcontractors' interests in the data.
(3) The government purpose rights period commences upon execution of the contract, subcontract, letter contract (or similar contractual instrument), contract modification, or option exercise that required the development. Upon expiration of the Government rights period, the Government has unlimited rights in the data including the right to authorize others to use the data for commercial purposes.
(4) During the government purpose rights period, the Government may not use, or authorize other persons to use, technical data marked with government purpose rights legends for commercial purposes. The Government shall not release or disclose data in which it has government purpose rights to any person, or authorize others to do so, unless--
(i) Prior to release or disclosure, the intended recipient is subject to the use and non-disclosure agreement at 227.7103-7; or
(ii) The intended recipient is a Government contractor receiving access to the data for performance of a Government contract that contains the clause at 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends.
(5) When technical data marked with government purpose rights legends will be released or disclosed to a Government contractor performing a contract that does not include the clause at 252.227-7025, the contract may be modified, prior to release or disclosure, to include that clause in lieu of requiring the contractor to complete a use and non-disclosure agreement.
(6) Contracting activities shall establish procedures to assure that technical data marked with government purpose rights legends are released or disclosed, including a release or disclosure through a Government solicitation, only to persons subject to the use and non-disclosure restrictions. Public announcements in the Commerce Business Daily or other publications must provide notice of the use and non-disclosure requirements. Class use and non-disclosure agreements (e.g., agreements covering all solicitations received by the XYZ company within a reasonable period) are authorized and may be obtained at any time prior to release or disclosure of the government purpose rights data. Documents transmitting government purpose rights data to persons under class agreements shall identify the technical data subject to government purpose rights and the class agreement under which such data are provided.
(c) Limited rights.
(1) The Government obtains limited rights in technical data--
(i) That pertain to items, components, or processes developed exclusively at private expense except when the Government is entitled to unlimited rights as provided in paragraphs (a)(2) and (a)(4) through (9) of this subsection; or
(ii) Created exclusively at private expense in the performance of a contract that does not require the development, manufacture, construction, or production of

items, components, or processes.
(2) Data in which the Government has limited rights may not be used, released, or disclosed outside the Government without the permission of the contractor asserting the restriction except for a use, release or disclosure that is-
-
(i) Necessary for emergency repair and overhaul; or
(ii) To a foreign government, other than detailed manufacturing or process data, when use, release, or disclosure is in the interest of the United States and is required for evaluational or informational purposes.
(3) The person asserting limited rights must be notified of the Government's intent to release, disclose, or authorize others to use such data prior to release or disclosure of the data except notification of an intended release, disclosure, or use for emergency repair or overhaul which shall be made as soon as practicable.
(4) When the person asserting limited rights permits the Government to release, disclose, or have others use the data subject to restrictions on further use, release, or disclosure, or for a release under paragraph (c)(2)(i) or (ii) of this subsection, the intended recipient must complete the use and non-disclosure agreement at 227.7103-7 prior to release or disclosure of the limited rights data.
(d) Specifically negotiated license rights.
(1) Negotiate specific licenses when the parties agree to modify the standard license rights granted to the Government or when the Government wants to obtain rights in data in which it does not have rights. When negotiating to obtain, relinquish, or increase the Government's rights in technical data, consider the acquisition strategy for the item, component, or process, including logistics support and other factors which may have relevance for a particular procurement. The Government may accept lesser rights when it has unlimited or government purpose rights in data but may not accept less than limited rights in such data. The negotiated license rights must stipulate what rights the Government has to release or disclose the data to other persons or to authorize others to use the data. Identify all negotiated rights in a license agreement made part of the contract.
(2) When the Government needs additional rights in data acquired with government purpose or limited rights, the contracting officer must negotiate with the contractor to determine whether there are acceptable terms for transferring such rights. Generally, such negotiations should be conducted only when there is a need to disclose the data outside the Government or if the additional rights are required for competitive reprocurement and the anticipated savings expected to be obtained through competition are estimated to exceed the acquisition cost of the additional rights. Prior to negotiating for additional rights in limited rights data, consider alternatives such as-
-
(i) Using performance specifications and form, fit, and function data to acquire or develop functionally equivalent items, components, or processes;
(ii) Obtaining a contractor's contractual commitment to qualify additional sources and maintain adequate competition among the sources; or
(iii) Reverse engineering, or providing items from Government inventories to contractors who request the items to facilitate the development of equivalent items through reverse engineering.

227.7103-6 Contract clauses.

(a) Use the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, in solicitations and contracts when the successful offeror(s) will be required to deliver technical data to the Government. Do not use the clause when the only deliverable items are computer software or computer software documentation (see 227.72), commercial items (see 227.7102-3), existing works (see 227.7105), special works (see 227.7106), or when contracting under the Small Business Innovation Research Program (see 227.7104). Except as provided in 227.7107-2, do not use the clause in architect-engineer and construction contracts.
(b) Use the clause at 252.227-7013 with its Alternate I in research contracts when the contracting officer determines, in consultation with counsel, that public dissemination by the contractor would be--
(1) In the interest of the Government; and
(2) Facilitated by the Government relinquishing its right to publish the work for sale, or to have others publish the work for sale on behalf of the Government.
(c) Use the clause at 252.227-7025, Limitations on the Use or Disclosure of Government Furnished Information Marked with Restrictive Legends, in solicitations and contracts when it is anticipated that the Government will provide the contractor, for performance of its contract, technical data marked with another contractor's restrictive legend(s).
(d) Use the provision at 252.227-7028, Technical Data or Computer Software Previously Delivered to the Government, in solicitations when the resulting contract will require the contractor to deliver technical data. The provision requires offerors to identify any technical data specified in the solicitation as deliverable data items that are the same or substantially the same as data items the offeror has delivered or is obligated to deliver, either as a contractor or subcontractor, under any other federal agency contract.
(e) Use the following clauses in solicitations and contracts that include the clause at 252.227-7013:
(1) 252.227-7015, Rights in Bid or Proposal Information;
(2) 252.227-7030, Technical Data - Withholding of Payment;
(3) 252.227-7036, Certification of Technical Data Conformity; and
(4) 252.227-7037, Validation of Restrictive Markings on Technical Data (paragraph (e) of the clause contains information that must be included in a challenge).

227.7103-7 Use and non-disclosure agreement.

(a) Except as provided in paragraph (b) of this subsection, technical data or computer software delivered to the Government with restrictions on use, modification, reproduction, release, performance, display, or disclosure may not be provided to third parties unless the intended recipient completes and signs the use and non-disclosure agreement at paragraph (c) of this subsection prior to release, or disclosure of the data.
(1) The specific conditions under which an intended recipient will be authorized to use, modify, reproduce, release, perform, display, or disclose technical data

subject to limited rights or computer software subject to restricted rights must be stipulated in an attachment to the use and non-disclosure agreement.

(2) For an intended release, disclosure, or authorized use of technical data or computer software subject to special license rights, modify paragraph (1)(d) of the use and non-disclosure agreement to enter the conditions, consistent with the license requirements, governing the recipient's obligations regarding use, modification, reproduction, release, performance, display or disclosure of the data or software.

(b) The requirement for use and non-disclosure agreements does not apply to Government contractors which require access to a third party's data or software for the performance of a Government contract that contains the clause at 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends.

(c) The prescribed use and non-disclosure agreement is:

Use and Non-Disclosure Agreement

The undersigned, _____(Insert Name)_____, an authorized representative of the _____(Insert Company Name)_____, (which is hereinafter referred to as the "Recipient") requests the Government to provide the Recipient with technical data or computer software (hereinafter referred to as "Data") in which the Government's use, modification, reproduction, release, performance, display or disclosure rights are restricted. Those Data are identified in an attachment to this Agreement. In consideration for receiving such Data, the Recipient agrees to use the Data strictly in accordance with this Agreement:

(1) The Recipient shall--

(a) Use, modify, reproduce, release, perform, display, or disclose Data marked with government purpose rights or SBIR data rights legends only for government purposes and shall not do so for any commercial purpose. The Recipient shall not release, perform, display, or disclose these Data, without the express written permission of the contractor whose name appears in the restrictive legend (the "Contractor"), to any person other than its subcontractors or suppliers, or prospective subcontractors or suppliers, who require these Data to submit offers for, or perform, contracts with the Recipient. The Recipient shall require its subcontractors or suppliers, or prospective subcontractors or suppliers, to sign a use and non-disclosure agreement prior to disclosing or releasing these Data to such persons. Such agreement must be consistent with the terms of this agreement.

(b) Use, modify, reproduce, release, perform, display, or disclose technical data marked with limited rights legends only as specified in the attachment to this Agreement. Release, performance, display, or disclosure to other persons is not authorized unless specified in the attachment to this Agreement or expressly permitted in writing by the Contractor. The Recipient shall promptly notify the Contractor of the execution of this Agreement and identify the Contractor's Data that has been or will be provided to the Recipient, the date and place the Data were or will be received, and the name and address of the Government office that has provided or will provide the Data.

(c) Use computer software marked with restricted rights legends only in performance of Contract Number _____(insert contract number(s))_____. The recipient shall not, for

example, enhance, decompile, disassemble, or reverse engineer the software; time share, or use a computer program with more than one computer at a time. The recipient may not release, perform, display, or disclose such software to others unless expressly permitted in writing by the licensor whose name appears in the restrictive legend. The Recipient shall promptly notify the software licensor of the execution of this Agreement and identify the software that has been or will be provided to the Recipient, the date and place the software were or will be received, and the name and address of the Government office that has provided or will provide the software.

(d) Use, modify, reproduce, release, perform, display, or disclose Data marked with special license rights legends (To be completed by the contracting officer. See 227.7103-7 (a)(2). Omit if none of the Data requested is marked with special license rights legends).

(2) The Recipient agrees to adopt or establish operating procedures and physical security measures designed to protect these Data from inadvertent release or disclosure to unauthorized third parties.

(3) The Recipient agrees to accept these Data "as is" without any Government representation as to suitability for intended use or warranty whatsoever. This disclaimer does not affect any obligation the Government may have regarding Data specified in a contract for the performance of that contract.

(4) The Recipient may enter into any agreement directly with the Contractor with respect to the use, modification, reproduction, release, performance, display, or disclosure of these Data.

(5) The Recipient agrees to indemnify and hold harmless the Government, its agents, and employees from every claim or liability, including attorneys fees, court costs, and expenses arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of Data received from the Government with restrictive legends by the Recipient or any person to whom the Recipient has released or disclosed the Data.

(6) The Recipient is executing this Agreement for the benefit of the Contractor. The Contractor is a third party beneficiary of this Agreement who, in addition to any other rights it may have, is intended to have the rights of direct action against the Recipient or any other person to whom the Recipient has released or disclosed the Data, to seek damages from any breach of this Agreement or to otherwise enforce this Agreement.

(7) The Recipient agrees to destroy these Data, and all copies of the Data in its possession, no later than 30 days after the date shown in paragraph (8) of this Agreement, to have all persons to whom it released the Data do so by that date, and to notify the Contractor that the Data have been destroyed.

(8) This Agreement shall be effective for the period commencing with the Recipient's execution of this Agreement and ending upon _____(Insert Date)_____. The obligations imposed by this Agreement shall survive the expiration or termination of the Agreement.

Recipient's Business Name _____

By_____ _____

Authorized Representative Date

Representative's Typed Name _____

and Title _____

(End of use and non-disclosure agreement)

227.7103-8 Deferred delivery and deferred ordering of technical data.

(a) Deferred delivery.

Use the clause at 252.227-7026, Deferred Delivery of Technical Data or Computer Software, when it is in the Government's interests to defer the delivery of technical data. The clause permits the contracting officer to require the delivery of technical data identified as "deferred delivery" data at any time until two years after acceptance by the Government of all items (other than technical data or computer software) under the contract or contract termination, whichever is later. The obligation of subcontractors or suppliers to deliver such technical data expires two years after the date the prime contractor accepts the last item from the subcontractor or supplier for use in the performance of the contract. The contract must specify which technical data is subject to deferred delivery. The contracting officer shall notify the contractor sufficiently in advance of the desired delivery date for such data to permit timely delivery.

(b) Deferred ordering.

Use the clause at 252.227-7027, Deferred Ordering of Technical Data or Computer Software, when a firm requirement for a particular data item(s) has not been established prior to contract award but there is a potential need for the data. Under this clause, the contracting officer may order any data that has been generated in the performance of the contract or any subcontract thereunder at any time until three years after acceptance of all items (other than technical data or computer software) under the contract or contract termination, whichever is later. The obligation of subcontractors to deliver such data expires three years after the date the contractor accepts the last item under the subcontract. When the data are ordered, the delivery dates shall be negotiated and the contractor compensated only for converting the data into the prescribed form, reproduction costs, and delivery costs.

227.7103-9 Copyright.

(a) Copyright license.

(1) The clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, requires a contractor to grant or obtain for the Government license rights which permit the Government to reproduce data, distribute copies of the data, publicly perform or display the data or, through the right to modify data, prepare derivative works. The extent to which the Government, and others acting on its behalf, may exercise these rights varies for each of the standard data rights licenses obtained under

the clause. When non-standard license rights in technical data will be negotiated, negotiate the extent of the copyright license concurrent with negotiations for the data rights license. Do not negotiate a copyright license that provides less rights than the standard limited rights license in technical data.

(2) The clause at 252.227-7013 does not permit a contractor to incorporate a third party's copyrighted data into a

deliverable data item unless the contractor has obtained an appropriate license for the Government and, when applicable, others acting on the Government's behalf, or has obtained the contracting officer's written approval to do so. Grant approval to use third party copyrighted data in which the Government will not receive a copyright license only when the Government's requirements cannot be satisfied without the third party material or when the use of the third party material will result in cost savings to the Government which outweigh the lack of a copyright license.

(b) Copyright considerations - acquisition of existing and special works.

See 227.7105 or 227.7106 for copyright considerations when acquiring existing or special works.

227.7103-10 Contractor identification and marking of technical data to be furnished

(a) Identification requirements.

(1) The solicitation provision at 252.227-7017, Identification and Assertion of Use, Release, or Disclosure Restrictions, requires offerors to identify to the contracting officer, prior to contract award, any technical data that the offeror asserts should be provided to the Government with restrictions on use, modification, reproduction, release or disclosure. This requirement does not apply to restrictions based solely on copyright. The notification and identification must be submitted as an attachment to the offer. If an offeror fails to submit the attachment or fails to complete the attachment in accordance with the requirements of the solicitation provision, such failure shall constitute a minor informality. Provide offerors an opportunity to remedy a minor informality in accordance with the procedures at FAR 14.405 or 15.607. An offeror's failure to correct the informality within the time prescribed by the contracting officer shall render the offer ineligible for award.

(2) The procedures for correcting minor informalities shall not be used to obtain information regarding asserted restrictions or an offeror's suggested asserted rights category. Questions regarding the justification for an asserted restriction or asserted rights category must be pursued in accordance with the procedures at 227.7103-13.

(3) The restrictions asserted by a successful offeror shall be attached to its contract unless, in accordance with the procedures at 227.7103-13, the parties have agreed that an asserted restriction is not justified. The contract attachment shall provide the same information regarding identification of the technical data, the asserted rights category, the basis for the assertion, and the name of the person asserting the restrictions as required by paragraph (d) of the solicitation provision at 252.227-7017. Subsequent

to contract award, the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, permits the contractor to make additional assertions under certain conditions. The additional assertions must be made in accordance with the procedures and in the format prescribed by that clause.

(4) Neither the pre- or post-award assertions made by the contractor, nor the fact that certain assertions are identified in the attachment to the contract, determine the respective rights of the parties. As provided at 227.7103-13,

the Government has the right to review, verify, challenge and validate restrictive markings.
(5) Information provided by offerors in response to the solicitation provision may be used in the source selection process to evaluate the impact on evaluation factors that may be created by restrictions on the Government's ability to use or disclose technical data. However, offerors shall not be prohibited from offering products for which the offeror is entitled to provide the Government limited rights in the technical data pertaining to such products and offerors shall not be required, either as a condition of being responsive to a solicitation or as a condition for award, to sell or otherwise relinquish any greater rights in technical data when the offeror is entitled to provide the technical data with limited rights.
(b) Contractor marking requirements.
The clause at 252.227-7013, Rights in Technical Data--Noncommercial Items--
(1) Requires a contractor that desires to restrict the Government's rights in technical data to place restrictive markings on the data, provides instructions for the placement of the restrictive markings, and authorizes the use of certain restrictive markings; and
(2) Requires a contractor to deliver, furnish, or otherwise provide to the Government any technical data in which the Government has previously obtained rights with the Government's pre-existing rights in that data unless the parties have agreed otherwise or restrictions on the Government's rights to use, modify, reproduce, release, perform, display, or disclose the data have expired. When restrictions are still applicable, the contractor is permitted to mark the data with the appropriate restrictive legend for which the data qualified.
(c) Unmarked technical data.
(1) Technical data delivered or otherwise provided under a contract without restrictive markings shall be presumed to have been delivered with unlimited rights and may be released or disclosed without restriction. To the extent practicable, if a contractor has requested permission (see paragraph (c)(2) of this subsection) to correct an inadvertent omission of markings, do not release or disclose the technical data pending evaluation of the request.
(2) A contractor may request permission to have appropriate legends placed on unmarked technical data at its expense. The request must be received by the contracting officer within six months following the furnishing or delivery of such data, or any extension of that time approved by the contracting officer. The person making the request must:
(i) Identify the technical data that should have been marked;
(ii) Demonstrate that the omission of the marking was inadvertent, the proposed marking is justified and conforms with the requirements for the marking of technical data contained in the clause at 252.227-7013; and
(iii) Acknowledge, in writing, that the Government has no liability with respect to any disclosure, reproduction, or use of the technical data made prior to the addition of the marking or resulting from the omission of the marking.
(3) Contracting officers should grant permission to mark only if the technical data were not distributed outside the Government or were distributed outside the Government with restrictions on further use or disclosure.

227.7103-11 Contractor procedures and records.

(a) The clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, requires a contractor, and its subcontractors or suppliers that will deliver technical data with other than unlimited rights, to establish and follow written procedures to assure that restrictive markings are used only when authorized and to maintain records to justify the validity of asserted restrictions on delivered data.
(b) The clause at 252.227-7037, Validation of Restrictive Markings on Technical Data requires contractors and their subcontractors at any tier to maintain records sufficient to justify the validity of restrictive markings on technical data delivered or to be delivered under a Government contract.

227.7103-12 Government right to establish conformity of markings.

(a) Nonconforming markings.
(1) Authorized markings are identified in the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items. All other markings are nonconforming markings. An authorized marking that is not in the form, or differs in substance, from the marking requirements in the clause at 252.227-7013 is also a nonconforming marking.
(2) The correction of nonconforming markings on technical data is not subject to 252.227-7037, Validation of Restrictive Markings on Technical Data. To the extent practicable, the contracting officer should return technical data bearing nonconforming markings to the person who has placed the nonconforming markings on such data to provide that person an opportunity to correct or strike the nonconforming marking at that person's expense. If that person fails to correct the nonconformity and return the corrected data within 60 days following the person's receipt of the data, the contracting officer may correct or strike the nonconformity at that person's expense. When it is impracticable to return technical data for correction, contracting officers may unilaterally correct any nonconforming markings at Government expense. Prior to correction, the data may be used in accordance with the proper restrictive marking.
(b) Unjustified markings.
(1) An unjustified marking is an authorized marking that does not depict accurately restrictions applicable to the Government's use, modification, reproduction, release, performance, display, or disclosure of the marked technical data. For example, a limited rights legend placed on technical data pertaining to items, components, or processes that were developed under a Government contract either exclusively at Government expense or with mixed funding (situations under which the Government obtains unlimited or government purpose rights) is an unjustified marking.
(2) Contracting officers have the right to review and challenge the validity of unjustified markings. However, at any time during performance of a contract and notwithstanding existence of a challenge, the contracting officer and the person who has asserted a restrictive marking may agree that the restrictive marking is not justified. Upon such agreement, the contracting officer may, at his or her election, either--

(i) Strike or correct the unjustified marking at that person's expense; or
(ii) Return the technical data to the person asserting the restriction for correction at that person's expense. If the data are returned and that person fails to correct or strike the unjustified restriction and return the corrected data to the contracting officer within 60 days following receipt of the data, the unjustified marking shall be corrected or stricken at that person's expense.

227.7103-13 Government right to review, verify, challenge and validate asserted res

(a) General.

An offeror's assertion(s) of restrictions on the Government's rights to use, modify, reproduce, release, or disclose technical data do not, by themselves, determine the extent of the Government's rights in the technical data. Under 10 U.S.C. 2321, the Government has the right to challenge asserted restrictions when there are reasonable grounds to question the validity of the assertion and continued adherence to the assertion would make it impractical to later procure competitively the item to which the data pertain.

(b) Pre-award considerations.

The challenge procedures required by 10 U.S.C. 2321 could significantly delay awards under competitive procurements. Therefore, avoid challenging asserted restrictions prior to a competitive contract award unless resolution of the assertion is essential for successful completion of the procurement.

(c) Challenge and validation.

Contracting officers must have reasonable grounds to challenge the current validity of an asserted restriction. Before issuing a challenge to an asserted restriction, carefully consider all available information pertaining to the assertion. All challenges must be made in accordance with the provisions of the clause at 252.227-7037, Validation of Restrictive Markings on Technical Data.

(1) Challenge period.

Asserted restrictions should be reviewed before acceptance of technical data deliverable under the contract. Assertions must be challenged within three years after

final payment under the contract or three years after delivery of the data, whichever is later. However, restrictive markings may be challenged at any time if the technical data--

(i) Are publicly available without restrictions;
(ii) Have been provided to the United States without restriction; or
(iii) Have been otherwise made available without restriction other than a release or disclosure resulting from the sale, transfer, or other assignment of interest in the technical data to another party or the sale or transfer of some or all of a business entity or its assets to another party.

(2) Pre-challenge requests for information.

(i) After consideration of the situations described in paragraph (c)(3) of this subsection, contracting officers may request the person asserting a restriction to furnish a written explanation of the facts and supporting documentation for the assertion in sufficient detail to enable the contracting officer to ascertain the basis of the

restrictive markings. Additional supporting documentation may be requested when the explanation provided by the person making the assertion does not, in the contracting officer's opinion, establish the validity of the assertion.
(ii) If the person asserting the restriction fails to respond to the contracting officer's request for information or additional supporting documentation, or if the information submitted or any other available information pertaining to the validity of a restrictive marking does not justify the asserted restriction, a challenge should be considered.
(3) Transacting matters directly with subcontractors.
The clause at 252.227-7037 obtains the contractor's agreement that the Government may transact matters under the clause directly with a subcontractor, at any tier, without creating or implying privity of contract. Contracting officers should permit a subcontractor or supplier to transact challenge and validation matters directly with the Government when--
(i) A subcontractor's or supplier's business interests in its technical data would be compromised if the data were disclosed to a higher tier contractor;
(ii) There is reason to believe that the contractor will not respond in a timely manner to a challenge and an untimely response would jeopardize a subcontractor's or supplier's right to assert restrictions; or
(iii) Requested to do so by a subcontractor or supplier.
(4) Challenge notice.
Do not issue a challenge notice unless there are reasonable grounds to question the validity of an assertion. Assertions may be challenged whether or not supporting documentation was requested from the person asserting the restriction. Challenge notices must be in writing and issued to the contractor or, after consideration of the situations described in paragraph (c)(3) of this subsection, the person asserting the restriction. The challenge notice must include the information in paragraph (e) of the clause at 252.227-7037.
(5) Extension of response time.
The contracting officer, at his or her discretion, may extend the time for response contained in a challenge notice, as appropriate, if the contractor submits a timely written request showing the need for additional time to prepare a response.
(6) Contracting officer's final decision.
Contracting officers must issue a final decision for each challenged assertion, whether or not the assertion has been justified.
(i) A contracting officer's final decision that an assertion is not justified must be issued as soon as practicable following the failure of the person asserting the restriction to respond to the contracting officer's challenge within 60 days, or any extension to that time granted by the contracting officer.
(ii) A contracting officer who, following a challenge and response by the person asserting the restriction, determines that an asserted restriction is justified, shall issue a final decision sustaining the validity of the asserted restriction. If the asserted restriction was made subsequent to submission of the contractor's offer, add the asserted restriction to the contract attachment.
(iii) A contracting officer who determines that the validity of an asserted restriction has not been justified shall issue a contracting officer's final decision within

the time frames prescribed in 252.227-7037. As provided in paragraph (g) of that clause, the Government is obligated to continue to respect the asserted restrictions through final disposition of any appeal unless the agency head notifies the person asserting the restriction that urgent or compelling circumstances do not permit the Government to continue to respect the asserted restriction.

(7) Multiple challenges to an asserted restriction.

When more than one contracting officer challenges an asserted restriction, the contracting officer who made the earliest challenge is responsible for coordinating the Government challenges. That contracting officer shall consult with all other contracting officers making challenges, verify that all challenges apply to the same asserted restriction and, after consulting with the contractor, subcontractor, or supplier asserting the restriction, issue a schedule that provides that person a reasonable opportunity to respond to each challenge.

(8) Validation.

Only a contracting officer's final decision, or actions of an agency board of contract appeals or a court of competent jurisdiction, that sustain the validity of an asserted restriction constitute validation of the asserted restriction.

227.7103-14 Conformity, acceptance, and warranty of technical data.

(a) Statutory requirements.

10 U.S.C. 2320--

(1) Requires contractors to furnish written assurance, at the time technical data are delivered or are made available to the Government, that the technical data are complete, accurate, and satisfy the requirements of the contract concerning such data;

(2) Provides for the establishment of remedies applicable to technical data found to be incomplete, inadequate, or not to satisfy the requirements of the contract concerning such data; and

(3) Authorizes agency heads to withhold payments (or exercise such other remedies an agency head considers appropriate) during any period if the contractor does not meet the requirements of the contract pertaining to the delivery of technical data.

(b) Conformity and acceptance.

(1) Solicitations and contracts requiring the delivery of technical data shall specify the requirements the data must satisfy to be acceptable. Contracting officers, or their authorized representatives, are responsible for determining whether technical data tendered for acceptance conform to the contractual requirements.

(2) The clause at 252.227-7030, Technical Data--Withholding of Payment, provides for withholding up to 10 percent of the contract price pending correction or replacement of the nonconforming technical data or negotiation of an equitable reduction in contract price. The amount subject to withholding may be expressed as a fixed dollar amount or as a percentage of the contract price. In either case, the amount shall be determined giving consideration to the relative value and importance of the data. For example--

(i) When the sole purpose of a contract is to produce the data, the relative value of that data may be considerably higher than the value of data produced under a contract where the production of the data is a secondary objective;

or
(ii) When the Government will maintain or repair items, repair and maintenance data may have a considerably higher relative value than data that merely describe the item or provide performance characteristics.
(3) Do not accept technical data that do not conform to the contractual requirements in all respects. Except for nonconforming restrictive markings (see paragraph (b)(4) of this subsection), correction or replacement of nonconforming data, or an equitable reduction in contract price when correction or replacement of the nonconforming data is not practicable or is not in the Government's interests, shall be accomplished in accordance with--
(i) The provisions of a contract clause providing for inspection and acceptance of deliverables and remedies for nonconforming deliverables; or
(ii) The procedures at FAR 46.407(c) through (g), if the contract does not contain an inspection clause providing remedies for nonconforming deliverables.
(4) Follow the procedures at 227.7103-12(a)(2) if nonconforming markings are the sole reason technical data fail to conform to contractual requirements. The clause at 252.227-7030 may be used to withhold an amount from payment, consistent with the terms of the clause, pending correction of the nonconforming markings.
(c) Warranty.
(1) The intended use of the technical data and the cost, if any, to obtain the warranty should be considered before deciding to obtain a data warranty (see FAR 46.703). The fact that a particular item, component, or process is or is not warranted is not a consideration in determining whether or not to obtain a warranty for the technical data that pertain to the item, component, or process. For example, a data warranty should be considered if the Government intends to repair or maintain an item and defective repair or maintenance data would impair the Government's effective use of the item or result in increased costs to the Government.
(2) As prescribed in 246.710, use the clause at 252.246-7001, Warranty of Data, and its alternates, or a substantially similar clause when the Government needs a specific warranty of technical data.

227.7103-15 Subcontractor rights in technical data.

(a) 10 U.S.C. 2320 provides subcontractors at all tiers the same protection for their rights in data as is provided to prime contractors. The clauses at 252.227-7013, Rights in Technical Data--Noncommercial Items, and 252.227-7037, Validation of Restrictive Markings on Technical Data, implement the statutory requirements.
(b) 10 U.S.C. 2321 permits a subcontractor to transact directly with the Government matters relating to the validation of its asserted restrictions on the Government's rights to use or disclose technical data. The clause at 252.227-7037 obtains a contractor's agreement that the direct transaction of validation or challenge matters with subcontractors at any tier does not establish or imply privity of contract. When a subcontractor or supplier exercises its right to transact validation matters directly with the Government, contracting officers shall deal directly with such persons, as provided at 227.7103-13 (c)(3).

(c) Require prime contractors whose contracts include the following clauses to include those clauses, without modification except for appropriate identification of the parties, in contracts with subcontractors or suppliers, at all tiers, who will be furnishing technical data for non-commercial items in response to a Government requirement:
(1) 252.227-7013, Rights in Technical Data--Noncommercial Items;
(2) 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends;
(3) 252.227-7028, Technical Data or Computer Software Previously Delivered to the Government; and
(4) 252.227-7037, Validation of Restrictive Markings on Technical Data.
(d) Do not require contractors to have their subcontractors or suppliers at any tier relinquish rights in technical data to the contractor, a higher tier subcontractor, or to the Government, as a condition for award of any contract, subcontract, purchase order, or similar instrument except for the rights obtained by the Government under the Rights in Technical Data--Noncommercial Items clause contained in the contractor's contract with the Government.

227.7103-16 Providing technical data to foreign governments, foreign contractors, o

Technical data may be released or disclosed to foreign governments, foreign contractors, or international organizations only if release or disclosure is otherwise permitted both by Federal export controls and other national security laws or regulations. Subject to such laws and regulations, the Department of Defense--
(a) May release or disclose technical data in which it has obtained unlimited rights to such foreign entities or authorize the use of such data by those entities; and
(b) Shall not release or disclose technical data for which restrictions on use, release, or disclosure have been asserted to foreign entities, or authorize the use of technical data by those entities, unless the intended recipient is subject to the same provisions as included in the use and non-disclosure agreement at 227.7103-7 and the requirements of the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, governing use, modification, reproduction, release, performance, display, or disclosure of such data have been satisfied.

227.7103-17 Overseas contracts with foreign sources.

(a) The clause at 252.227-7032, Rights in Technical Data and Computer Software (Foreign), may be used in contracts with foreign contractors to be performed overseas, except Canadian purchases (see paragraph (c) of this subsection), in lieu of the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, when the Government requires the unrestricted right to use, modify, reproduce, perform, display, release or disclose all technical data to be delivered under the contract. Do not use the clause in contracts for existing or special works.
(b) When the Government does not require unlimited rights, the clause at 252.227-7032 may be modified to accommodate

the needs of a specific overseas procurement situation. The Government should obtain rights in the technical data that are not less than the rights the Government would have obtained under the data rights clause(s) prescribed in this part for a comparable procurement performed within the United States or its possessions.

(c) Contracts for Canadian purchases shall include the appropriate data rights clause prescribed in this part for a comparable procurement performed within the United States or its possessions.

227.7104 Contracts under the Small Business Innovation Research (SBIR) Program.

(a) Use the clause at 252.227-7018, Rights in Noncommercial Technical Data and Computer Software--Small Business Innovation Research (SBIR) Program, when technical data or computer software will be generated during performance of contracts under the SBIR program.

(b) Under the clause at 252.227-7018, the Government obtains a royalty-free license to use technical data marked with an SBIR data rights legend only for government purposes during the period commencing with contract award and ending five years after completion of the project under which the data were generated. Upon expiration of the five-year restrictive license, the Government has unlimited rights in the SBIR data. During the license period, the Government may not release or disclose SBIR data to any person other than its support services contractors except--

(1) For evaluational purposes;

(2) As expressly permitted by the contractor; or

(3) A use, release, or disclosure that is necessary for emergency repair or overhaul of items operated by the Government.

(c) Do not make any release or disclosure permitted by paragraph (b) of this section unless, prior to release or disclosure, the intended recipient is subject to the use and non-disclosure agreement at 227.7103-7.

(d) Use the clause at 252.227-7018 with its Alternate I in research contracts when the contracting officer determines, in consultation with counsel, that public dissemination by the contractor would be--

(1) In the interest of the Government; and

(2) Facilitated by the Government relinquishing its right to publish the work for sale, or to have others publish the work for sale on behalf of the Government.

(e) Use the following provision and clauses in SBIR solicitations and contracts that include the clause at 252.227-7018:

(1) 252.227-7016, Rights in Bid or Proposal Information;

(2) 252.227-7017, Identification and Assertion of Use, Release, or Disclosure Restrictions;

(3) 252.227-7019, Validation of Asserted Restrictions--Computer Software;

(4) 252.227-7030, Technical Data--Withholding of Payment;

(5) 252.227-7036, Certification of Technical Data Conformity; and

(6) 252.227-7037, Validation of Restrictive Markings on Technical Data (paragraph (e) of the clause contains information that must be included in a challenge).

(f) Use the following clauses and provision in SBIR solicitations and contracts in accordance with the guidance at 227.7103-6(c) and (d):

(1) 252.227-7025, Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends; and
(2) 252.227-7028, Technical Data or Computer Software Previously Delivered to the Government.

227.7105 Contracts for the acquisition of existing works.

227.7105-1 General.

(a) Existing works include motion pictures, television recordings, video recordings, and other audiovisual works in any medium; sound recordings in any medium; musical, dramatic, and literary works; pantomimes and choreographic works; pictorial, graphic, and sculptural works; and works of a similar nature. Usually, these or similar works were not first created, developed, generated, originated, prepared, or produced under a Government contract. Therefore, the Government must obtain a license in the work if it intends to reproduce the work, distribute copies of the work, prepare derivative works, or perform or display the work publicly. When the Government is not responsible for the content of an existing work, it should require the copyright owner to indemnify the Government for liabilities that may arise out of the content, performance, use, or disclosure of such data.
(b) Follow the procedures at 227.7106 for works which will be first created, developed, generated, originated, prepared, or produced under a Government contract and the Government needs to control distribution of the work or has a specific need to obtain indemnity for liabilities that may arise out of the creation, content, performance, use, or disclosure of the work or from libelous or other unlawful material contained in the work. Follow the procedures at 227.7103 when the Government does not need to control distribution of such works or obtain such indemnities.

227.7105-2 Acquisition of existing works without modification.

(a) Use the clause at 252.227-7021, Rights in Data--Existing Works, in lieu of the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, in solicitations and contracts exclusively for existing works when--
(1) The existing works will be acquired without modification; and
(2) The Government requires the right to reproduce, prepare derivative works, or publicly perform or display the existing works; or
(3) The Government has a specific need to obtain indemnity for liabilities that may arise out of the content, performance, use, or disclosure of such data.
(b) The clause at 252.227-7021 provides the Government, and others acting on its behalf, a paid-up, non-exclusive, irrevocable, world-wide license to reproduce, prepare derivative works and publicly perform or display the works called for by a contract and to authorize others to do so for government purposes.

(c) A contract clause is not required to acquire existing works such as books, magazines and periodicals, in any storage or retrieval medium, when the Government will not reproduce the books, magazines or periodicals, or prepare derivative works.

227.7105-3 Acquisition of modified existing works.

Use the clause at 252.227-7020, Rights in Special Works, in solicitations and contracts for modified existing works in lieu of the clause at 252.227-7021, Rights in Data--Existing Works.

227.7106 Contracts for special works.

(a) Use the clause at 252.227-7020, Rights in Special Works, in solicitations and contracts where the Government has a specific need to control the distribution of works first produced, created, or generated in the performance of a contract and required to be delivered under that contract, including controlling distribution by obtaining an assignment of copyright, or a specific need to obtain indemnity for liabilities that may arise out of the creation, delivery, use, modification, reproduction, release, performance, display, or disclosure of such works. Use the clause--

(1) In lieu of the clause at 252.227-7013, Rights in Technical Data--Noncommercial Items, when the Government must own or control copyright in all works first produced, created, or generated and required to be delivered under a contract; or

(2) In addition to the clause at 252.227-7013 when the Government must own or control copyright in a portion of a work first produced, created, or generated and required to be delivered under a contract. The specific portion in which the Government must own or control copyright must be identified in a special contract requirement.

(b) Although the Government obtains an assignment of copyright and unlimited rights in a special work under the clause at 252.227-7020, the contractor retains use and disclosure rights in that work. If the Government needs to restrict a contractor's rights to use or disclose a special work, it must also negotiate a special license which specifically restricts the contractor's use or disclosure rights.

(c) The clause at 252.227-7020 does not permit a contractor to incorporate into a special work any works copyrighted by others unless the contractor obtains the contracting officer's permission to do so and obtains for the Government a non-exclusive, paid up, world-wide license to make and distribute copies of that work, to prepare derivative works, to perform or display publicly any portion of the work, and to permit others to do so for government purposes. Grant permission only when the Government's requirements cannot be satisfied unless the third party work is included in the deliverable work.

(d) Examples of works which may be procured under the Rights in Special Works clause include, but are not limited, to audiovisual works, computer data bases, computer software documentation, scripts, soundtracks, musical compositions,

and adaptations; histories of departments, agencies, services or units thereof; surveys of Government establishments; instructional works or guidance to Government officers and employees on the discharge of their official duties; reports, books, studies, surveys or similar documents; collections of data containing information pertaining to individuals that, if disclosed, would violate the right of privacy or publicity of the individuals to whom the information relates; or investigative reports.

227.7107 Contracts for architect-engineer services.

This section sets forth policies and procedures, pertaining to data, copyrights, and restricted designs unique to the acquisition of construction and architect-engineer services.

227.7107-1 Architectural designs and data clauses for architect-engineer or constru

(a) Except as provided in paragraph (b) of this subsection and in 227.7107-2, use the clause at 252.227-7022, Government Rights (Unlimited), in solicitations and contracts for architect-engineer services and for construction involving architect-engineer services.
(b) When the purpose of a contract for architect-engineer services, or for construction involving architect-engineer services, is to obtain a unique architectural design of a building, a monument, or construction of similar nature, which for artistic, aesthetic or other special reasons the Government does not want duplicated, the Government may acquire exclusive control of the data pertaining to the design by including the clause at 252.227-7023, Drawings and Other Data to Become Property of Government, in solicitations and contracts.
(c) The Government shall obtain unlimited rights in shop drawings for construction. In solicitations and contracts calling for delivery of shop drawings, include the clause at 252.227-7033, Rights in Shop Drawings.

227.7107-2 Contracts for construction supplies and research and development work.

Use the provisions and clauses required by 227.7103-6 and 227.7203-6 when the acquisition is limited to--
(a) Construction supplies or materials;
(b) Experimental, developmental, or research work, or test and evaluation studies of structures, equipment, processes, or materials for use in construction; or
(c) Both.

227.7107-3 Approval of restricted designs.

The clause at 252.227-7024, Notice and Approval of Restricted Designs, may be included in architect-engineer contracts to permit the Government to make informed decisions concerning noncompetitive aspects of the design.

227.7108 Contractor data repositories.

(a) Contractor data repositories may be established when permitted by agency procedures. The contractual instrument establishing the data repository must require, as a minimum, the data repository management contractor to--

(1) Establish and maintain adequate procedures for protecting technical data delivered to or stored at the repository from unauthorized release or disclosure;

(2) Establish and maintain adequate procedures for controlling the release or disclosure of technical data from the repository to third parties consistent with the Government's rights in such data;

(3) When required by the contracting officer, deliver data to the Government on paper or in other specified media;

(4) Be responsible for maintaining the currency of data delivered directly by Government contractors or subcontractors to the repository;

(5) Obtain use and non-disclosure agreements (see 227.7103-7) from all persons to whom government purpose rights data is released or disclosed; and

(6) Indemnify the Government from any liability to data owners or licensors resulting from, or as a consequence of, a release or disclosure of technical data made by the data repository contractor or its officers, employees, agents, or representatives.

(b) If the contractor is or will be the data repository manager, the contractor's data management and distribution responsibilities must be identified in the contract or the contract must reference the agreement between the Government and the contractor that establishes those responsibilities.

(c) If the contractor is not and will not be the data repository manager, do not require a contractor or subcontractor to deliver technical data marked with limited rights legends to a data repository managed by another contractor unless the contractor or subcontractor who has asserted limited rights agrees to release the data to the repository or has authorized, in writing, the Government to do so.

(d) Repository procedures may provide for the acceptance, delivery, and subsequent distribution of technical data in storage media other than paper, including direct electronic exchange of data between two computers. The procedures must provide for the identification of any portions of the data provided with restrictive legends, when appropriate. The acceptance criteria must be consistent with the authorized delivery format.

This Page Intentionally Left Blank

EO 12923

This Page Intentionally Left Blank

Continuation Of Export Control Regulations

The White House
Office of the Press Secretary

For Immediate Release June 30, 1994

Executive Order
#12923
- - - - - - - - - - - -

Continuation Of **Export Control** Regulations

By the authority vested in me as President by the Constitution and the laws of the United States of America, including but not limited to section 203 of the International Emergency Economic Powers Act ("Act") (50 U.S.C. 1702), I, William J. Clinton, President of the United States of America, find that the unrestricted access of foreign parties to U.S. goods, technology, and technical data and the existence of certain boycott practices of foreign nations, in light of the expiration of the **Export** Administration Act of 1979, as amended (50 U.S.C. App. 2401 et seq.), constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States and hereby declare a national emergency with respect to that threat.

Accordingly, in order (a) to exercise the necessary vigilance with respect to **exports** and activities affecting the national security of the United States; (b) to further significantly the foreign policy of the United States, including its policy with respect to cooperation by U.S. persons with certain foreign boycott activities, and to fulfill its international responsibilities; and (c) to protect the domestic economy from the excessive drain of scarce materials and reduce the serious economic impact of foreign demand, it is hereby ordered as follows:

Section 1. To the extent permitted by law, the provisions of the **Export** Administration Act of 1979, as amended, and the provisions for administration of the **Export** Administration Act of 1979, as amended, shall be carried out under this order so as to continue in full force and effect and amend, as necessary, the **export control** system heretofore maintained by the **Export** Administration Regulations issued under the **Export** Administration Act of 1979, as amended. The delegations of authority set forth in Executive Order No. 12002 of July 7, 1977, as amended by Executive Order No. 12755 of March 12, 1991; Executive Order No. 12214 of May 2, 1980; Executive Order No. 12735 of November 16, 1990; and Executive Order No. 12851 of June 11, 1993, shall be incorporated in this order and shall apply to the exercise of authorities under this order.

Sec. 2. All rules and regulations issued or contained in effect by the Secretary of Commerce under the authority of the **Export** Administration Act of 1979, as amended, including those published in Title 15, Subtitle B, Chapter Vii, Subchapter C, of the Code of Federal Regulations, Parts 768 through 799, and all orders, regulations, licenses, and other forms of administrative action issued, taken, or continued in effect pursuant thereto, shall, until amended or revoked by the Secretary of Commerce, remain in full force and effect as if issued or taken pursuant to this order, except that the provisions of sections 203(b)(2) and 206 of the Act (50 U.S.C. 1702(b)(2) and 1705) shall control over any inconsistent provisions in the regulations. Nothing in this section shall affect the continued applicability of administrative sanctions provided for by the regulations described above.

Sec. 3. Provisions for administration of section 38(e) of the Arms **Export Control** Act (22 U.S.C. 2778(e)) may be made and shall continue in full force and effect until amended or revoked under the authority of section 203 of the Act (50 U.S.C. 1702). To the extent permitted by law, this order also shall constitute authority for the issuance and continuation in full force and effect of all rules and regulations by the President or his delegate, and all orders, licenses, and other forms of administrative actions issued, taken, or continued in effect pursuant thereto, relating to the administration of section38(e).

Sec. 4. This order shall be effective as of midnight between June 30, 1994, and July 1, 1994, and shall remain in effect until terminated. It is my intention to terminate this order upon the enactment into law of a bill reauthorizing the authorities contained in the **Export** Administration Act.

William J. Clinton

The White House,
June 30, 1994.

Continuation Of Export Control Regulations
To comment on this service: feedback@www.whitehouse.gov 2/17/97

Arms Export Control Act

This Page Intentionally Left Blank

2751.00 Need for international defense cooperation and military export controls; Presidential waiver; report to Congress; arms sales policy

As declared by the Congress in the Arms Control and Disarmament Act (22 U.S.C. 2551 et seq.), an ultimate goal of the United States continues to be a world which is free from the scourge of war and the dangers and burdens of armaments; in which the use of force has been subordinated to the rule of law; and in which international adjustments to a changing world are achieved peacefully. In furtherance of that goal, it remains the policy of the United States to encourage regional arms control and disarmament agreements and to discourage arms races.

The Congress recognizes, however, that the United States and other free and independent countries continue to have valid requirements for effective and mutually beneficial defense relationships in order to maintain and foster the environment of international peace and security essential to social, economic, and political progress. Because of the growing cost and complexity of defense equipment, it is increasingly difficult and uneconomic for any country, particularly a developing country, to fill all of its legitimate defense requirements from its own design and production base. The need for international defense cooperation among the United States and those friendly countries to which it is allied by mutual defense treaties is especially important, since the effectiveness of their armed forces to act in concert to deter or defeat aggression is directly related to the operational compatibility of their defense equipment.

Accordingly, it remains the policy of the United States to facilitate the common defense by entering into international arrangements with friendly countries which further the objective of applying agreed resources of each country to programs and projects of cooperative exchange of data, research, development, production, procurement, and logistics support to achieve specific national defense requirements and objectives of mutual concern. To this end, this chapter authorizes sales by the United States Government to friendly countries having sufficient wealth to maintain and equip their own military forces at adequate strength, or to assume progressively larger shares of the costs thereof, without undue burden to their economies, in accordance with the restraints and control measures specified herein and in furtherance of the security objectives of the United States and of the purposes and principles of the United Nations Charter.

It is the sense of the Congress that all such sales be approved only when they are consistent with the foreign policy interests of the United States, the purposes of the foreign assistance program of the United States as embodied in the Foreign Assistance Act of 1961, as amended (22 U.S.C. 2151 et seq.), the extent and character of the military requirement, and the economic and financial capability of the recipient country, with particular regard being given, where appropriate, to proper balance among such sales, grant military assistance, and economic assistance as well as to the impact of the sales on programs of social and economic development and on existing or incipient arms races.

It shall be the policy of the United States to exert leadership in the world community to bring about arrangements for reducing the international trade in implements of war and to lessen the danger of outbreak of regional conflict and the burdens of armaments. United States programs for or procedures governing the export, sale, and grant of defense articles and defense services to foreign countries and international organizations shall be administered in a manner which will carry out this policy.

It is the sense of the Congress that the President should seek to initiate multilateral discussions for the purpose of reaching agreements among the principal arms suppliers and arms purchasers and other countries with respect to the control of the international trade in armaments. It is further the sense of Congress that the President should work actively with all nations to check and control the international

sale and distribution of conventional weapons of death and destruction and to encourage regional arms control arrangements. In furtherance of this policy, the President should undertake a concerted effort to convene an international conference of major arms-supplying and arms-purchasing nations which shall consider measures to limit conventional arms transfers in the interest of international peace and stability.

It is the sense of the Congress that the aggregate value of defense articles and defense services -

(1) which are sold under section 2761 or section 2762 of this title; or
(2) which are licensed or approved for export under section 2778 of this title to, for the use, or for benefit of the armed forces, police, intelligence, or other internal security forces of a foreign country or international organization under a commercial sales contract; in any fiscal year should not exceed current levels.

It is the sense of the Congress that the President maintain adherence to a policy of restraint in conventional arms transfers and that, in implementing this policy worldwide, a balanced approach should be taken and full regard given to the security interests of the United States in all regions of the world and that particular attention should be paid to controlling the flow of conventional arms to the nations of the developing world. To this end, the President is encouraged to continue discussions with other arms suppliers in order to restrain the flow of conventional arms to less developed countries.